(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 March 2002 (07.03.2002)

PCT

(10) International Publication Number
WO 02/19614 A1

(51) International Patent Classification[7]: H04L 9/32, 29/06, G06F 17/60

(21) International Application Number: PCT/IN01/00102

(22) International Filing Date: 21 May 2001 (21.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/650,433 29 August 2000 (29.08.2000) US

(71) Applicant: **MYESPACE.NET PRIVATE LIMITED** [IN/IN]; Greams Dugar, 3rd Floor, 149 Greams Road, Chennai 600 006, Tamil Nadu (IN).

(72) Inventor: **CHANDRAMOULI, Balaraman**; Greams Dugar, 3rd Floor, 149 Greams Road, Chennai 600 006, Tamil Nadu (IN).

(74) Agents: **DEPENNING, R., G.** et al.; Depenning & Depenning, 31 South Bank Road, Chennai 600028 (IN).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/19614 A1

(54) Title: METHOD AND SYSTEM FOR AUTHENTICATING E-COMMERCE TRANSACTION

(57) Abstract: A method and system for authorizing/authenticating E-commerce transactions is provided. The process registers a user and service providers for conducting secured on-line electronic commerce transactions. To register the user, profile information is entered and a telephone call is initiated. The user is prompted to enter an authentication code and thereafter, the user enters the authentication code. The user specific authentication code is then stored in a database. Thereafter the registered user can request to conduct an E-commerce transaction with the service provider that is also registered with an authorization /authentication module. The authorization/authentication module generates a transaction identification number upon receiving the user's request and initiates a telephone call to the user. Thereafter the user is prompted to enter the authentication code and the transaction identification number for verifying user identity. The entered authentication numbers compared with stored authentication number.

METHOD AND SYSTEM FOR AUTHENTICATING E-COMMERCE TRANSACTION

FIELD OF THE INVENTION

The invention relates to a method and system for authenticating E-commerce transaction.

Appendix "A" and "B" attached to this specification contain source code in HTML, Java, Java script, Visual basic programming language for programming a computer, are a part of the present disclosure, and are incorporated by reference in their entirety.

A portion of the disclosure of this patent document contains material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the patent and trademark office patent files or records, but otherwise reserves all copyright whatsoever.

The internet connects thousands of computers world wide through well-known protocols, for example, Transmission Control Protocol (TCP)/Internet Protocol (IP), into a vast network.

Information on the Internet is stored world wide as computer files, mostly written in the Hypertext Mark Up Language ("HTML"). The collection of all such publicly available computer files is known as the World Wide Web (WWW).

The WWW is a multimedia-enabled hypertext system used for navigating the Internet and is made up of hundreds of thousands of web pages with images and text and video files, which can be displayed on a computer monitor. Each web page can have connections to other pages, which may be located on any computer connected to the Internet.

A typical Internet user uses a client program called a "Web Browser" to connect to the Internet. A user can connect to the Internet via a proprietary network, such as America Online or CompuServe, or via an Internet Service Provider, e.g., Earthlink.

A Web Browser may run on any computer connected to the Internet. Currently, various browsers are available of which two prominent browsers are Netscape Navigator™ and Microsoft Internet Explorer™ . The Web Browser receives and sends requests to a web server and acquires information from the WWW. A web

server is a program that, upon receipt of a request, sends the requested data to the requesting user.

A standard naming convention known as Uniform Resource Locator ("URL") has been adopted to represent hypermedia links and links to network services. Most files or services can be represented with a URL. URLs enable Web Browsers to go directly to any file held on any WWW server.

Information from the WWW is accessed using well-known protocols, including the Hypertext Transport Protocol ("HTTP"), the Wide Area Information Service ("WAIS") and the File Transport Protocol ("FTP"), over TCP/IP protocol. The transfer format for standard WWW pages is Hypertext Transfer Protocol (HTTP).

The advent and progress of the Internet has changed the way consumers shop. A consumer today can buy numerous products and services via the Internet. A typical electronic commerce transaction ("E-commerce") involves the following steps: (a) a consumer logs onto a merchant's website, (b) selects products and/or services, (c) pays via credit or debit card or other electronic

means, and (d) the transaction is completed, and thereafter products and/or services are delivered and/or performed.

E-commerce transactions today have gained considerable popularity among consumers and businesses. However, the security for E-commerce transactions is still questionable. Typically, a consumer uses a user identification number ("user ID.") and user specified password to execute an E-commerce transaction. However, if an unauthorized user accesses the user ID and password, then the current security systems will fail to prevent an unauthorized E-commerce transaction. Hence consumers and businesses can potentially loose millions of dollars because the conventional security systems in E-commerce do not have an efficient authorization and authentication process.

Therefore, what is needed is a method and system for authenticating and authorizing E-commerce transactions that can enhance security for conventional E-commerce transactions.

SUMMARY

The present invention solves the foregoing drawbacks by providing a method and system for authorizing/authenticating

E-commerce transactions. Before allowing a user to proceed with an E-commerce transaction, the process registers the user with a central registry. The user enters user information, which is then received by the registry. The user may enter user information in a web browser and transmit the information to the registry via the Internet, the main channel for the E-commerce transaction.

After the registry receives the profile information, under the registration process, the registry initiates a call to a user designated personal device, for example, a mobile telephone or a land phone etc. It is noteworthy that the user designated device is based upon an alternate channel separate from the main E-commerce transaction channel. The user is prompted to enter an authentication code. The user enters the authentication code, which is then stored in the database, and the user is registered.

According to the present invention, the service provider that provides goods and/or services to the user is also registered with the registry. Under one aspect of the present system, a registered user can request an E-commerce transaction with a registered service provider.

The registry receives a user transaction request to proceed with an E-commerce transaction. Such a request is received from the main E-commerce transaction channel, generally through a web browser. The registry generates a transaction identification number upon receiving the user's request. The transaction identification number is sent to the user via the main E-commerce transaction channel. The registry initiates a call to a user designated personal device, for example, a mobile telephone or a land phone etc. It is noteworthy that the user-designated device is based upon an alternate channel separate from the main E-commerce transaction channel. Thereafter the user is prompted to enter an authentication code and the transaction identification number for verifying user identity. A cell phone, a mobile telephone or a land phone may be used to receive the telephone call and enter the authentication code. Other devices for example a two-way pager and smart cards etc. may also be used to enter the authentication code.

The user enters the authentication code and the transaction identification number. User entered authentication code is compared with user specific stored authentication code. User entered transaction identification number is also compared with the generated transaction identification number. If both the numbers match, user identity is authenticated, and the user is authorized to

proceed with the requested transaction. Authorization data including transaction identification number, date and time of transaction, and the IP address of the device that is connected to the main channel are stored.

One advantage of the present invention is that initiation and authentication of an E-commerce transaction requires two different channels The main channel provides security for the user to request a transaction and obtain a transaction identification number. The alternate channel assists in authentication. In order to breach the system of the present invention, one will have to know the user login identity and password on the main channel, personal device details, authentication code on the alternate channel, transaction identification number on the main channel and know the algorithm used for encrypting all the data during the transaction. The probability of simultaneously acquiring all the foregoing data is quite remote. Hence the present invention provides a secure system for E-commerce transactions.

Another advantage of the present process is that a user must enter an authentication code for registration via an alternative channel and device, e.g., a cell, mobile or land phone, two-way pager or smart cards etc. Hence even if user password is stolen, the

authentication code is still required to proceed with a transaction. This additional channel (authentication code and transaction identification number) provides an extra layer of security for vulnerable E-commerce transactions.

Yet another advantage of the present system is that a user must enter two sets of numbers, one transaction specific, i.e., the transaction identification number, and another user specific, i.e., the authentication code. Since the user must be identified prior to any transaction by entering the authentication code via an alternate channel other than the main E-commerce transaction channel, it provides a degree of security that is much more stringent than identifying the user by merely a password.

Yet another advantage of the present system is that users can authenticate themselves via a mobile phone. Hence the system is flexible.

Yet another advantage of the present invention is that the authentication code is entered on a device (e.g. cell phone or land phone etc.) specified by the user.

Yet another advantage of the present invention is that any transaction authorized by registry is stored for future reference. Hence any claims by the user or a third party against authorized transaction can be repudiated by the stored authorization data.

This brief summary has been provided so that the nature of the invention may be understood quickly. A more complete understanding of the invention can be obtained by reference to the following detailed description of the preferred embodiments thereof in connection with the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a computing system to carry out the inventive technique.

Figure 2 is a block diagram of the architecture of the computing system of Fig. 1.

Figure 3 is a block diagram of the Internet Topology.

Figure 4A is a block diagram of the architecture of a system, according to the present invention.

Figure 4B is a block diagram of a registry module according to the present system.

Figure 4C is a block diagram of the architecture showing a Service point coupled to the registry module, according to the present invention.

Figure 5A is a flow diagram showing process steps for registering users.

Figure 5B is a flow diagram showing process steps for registering service providers.

Figure 6 is flow diagram of process steps for authorizing and authenticating an E-commerce transaction according to the present invention.

The use of similar reference numerals in different Figures indicates similar or identical items.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 is a block diagram of a computing system 10 for executing computer executable process steps according to one embodiment of the present invention. A consumer conducting an E-commerce transaction may use the computing system of Figure 1. Computing system 10 is connected to the main E-commerce transaction channel (Internet). It is noteworthy that the Figure 1 block diagram is not limiting and merely illustrative. Other devices that allow E-commerce transactions may be used to implement the methods and systems of the present invention. For example, laptops, notebook computers, a handheld device like the Palm-Pilot™ , digital or WebTV T ™ or a remote wireless device that can be connected to the Internet or another computer network that allows E-commerce transactions may be used instead of the computing system of Figure 1. Computing System 10 may also be used to host the authorization/authentication system according to the present invention.

Figure 1 includes a host computer 10 and a monitor 11. Monitor 11 may be a CRT type, a LCD type, or any other type of color or monochrome display. Also provided with computer 10 is a

keyboard 13 for entering text data and user commands, and a pointing device 14 for processing objects displayed on monitor 11.

Computer 10 includes a computer-readable memory medium such as a rotating disk 15 for storing readable data. Besides other programs, disk 15 can store application programs including web browsers by which computer 10 connects to the Internet and the systems described below, according to one aspect of the present invention.

Computer 10 can also access a computer-readable floppy disk storing data files, application program files, and computer executable process steps embodying the present invention or the like via a floppy disk drive 16. A CD-ROM interface (not shown) may also be provided with computer 10 to access application program files, audio files and data files stored on a CD-ROM.

A modem, an integrated services digital network (ISDN) connection, or the like also provides computer 10 with an Internet connection 12 to the World Wide Web (WWW). The Internet connection 12 allows computer 10 to download data files, audio files, application program files and conduct E-commerce

transactions. Internet connection 12 provides access to the main E-commerce transaction channel.

Computer 10 is also provided with external audio speakers 17A and 17B to assist a consumer to listen to any audio files. It is noteworthy that a listener may use headphones instead of audio speakers 17A and 17B to listen to any audio files.

Figure 2 is a block diagram showing the internal functional architecture of computer 10. As shown in Fig. 2, computer 10 includes a CPU 201 for executing computer-executable process steps and interfaces with a computer bus 208. Also shown in Figure 2 are a WWW interface 202, a display device interface 203, a keyboard interface 204, a pointing device interface 205, an audio interface 209, and a rotating disk 15. Audio Interface 209 allows a listener to listen to music, On-line (downloaded using the Internet or a private network) or off-line (using a CD).

As described above, disk 15 stores operating system program files, application program files, web browsers, and other files. Some of these files are stored on disk 15 using an installation program. For example, CPU 201 executes computer-executable

process steps of an installation program so that CPU 201 can properly execute the application program.

A random access main memory ("RAM") 206 also interfaces to computer bus 208 to provide CPU 201 with access to memory storage. When executing stored computer-executable process steps from disk 15 (or other storage media such as floppy disk 16 or WWW connection 12), CPU 201 stores and executes the process steps out of RAM 206.

Read only memory ("ROM") 207 is provided to store invariant instruction sequences such as start-up instruction sequences or basic input/output operating system (BIOS) sequences for operation of keyboard 13.

Figure 3 shows a typical topology of a computer network with computers similar to computer 10, connected to the Internet. For illustration purposes, three computers X, Y and Z are shown connected to the Internet 302 via Web interface 202 through a gateway 301, where gateway 301 can interface N number of computers. Web interface 202 may be a modem, network interface card or a unit for providing connectivity to other computer systems over a network using protocols such as X.25, Ethernet or TCP/IP,

or any device that allows, directly or indirectly, computer-to-computer communications.

It is noteworthy that the invention is not limited to a particular number of computers. Any number of computers that can be connected to the Internet 302 or any other computer network may be used.

Figure 3 further shows a second gateway 303 that connects a network of web servers 304 and 305 to the Internet 302. Web servers 304 and 305 may be connected with each other over a computer network. Web servers 304 and 305 can also facilitate provide E-commerce transactions, according to the present invention. Web servers 304 and 305 can also host the present system that secures E-Commerce transactions. Also shown in Figure 3 is a client side web server 308 that can be provided by an Internet service provider.

Figure 4A is a block diagram of the architecture, according to one embodiment of the present invention. A user's terminal 401 communicates with a registry 402. Terminal 401 may be similar to computer 10, laptop computer, a notebook computer, digital TV or

WebTV ™ a hand held device or similar device that can be connected to the Internet or another network.

Registry 402 may reside at a web server 304. A user inputs user specific information via terminal 401 and the user information is transferred to registry 402.

Figure 4B shows a block diagram of registry module 402 that includes receiving module 403A that receives requests from user terminal 401. Receiving module 403A also communicates with a database 403B either to store user information or search for user information.

Receiving module 403A also communicates with interactive Voice Response System ("IVR") 903C that can contact the user via an alternate channel 403D (not shown). Alternate channel 403D may allow a connection to a mobile or land phone, or two way pagers, and/or other devices. One example of IVR 403 C is sold by Dialogic Corporation 1515 Route 10, Parsippany, NJ 07054, Part number D/21H, which is a High Performance 2 Port voice processing board. It is noteworthy that the invention is not limited to the foregoing IVR 403 as sold by Dialogic Corporation, other comparable or similar voice processing boards and/or software

modules may be used to practice the embodiments under the present invention. IVR 403C is used to contact a user for authenticating an E-commerce transaction, as described below.

Figure 4C is a block diagram showing a service point 404 that communicates with registry 402. Service point 404 allows a user via user terminal 401 to conduct an E-commerce transaction. Service point 404 may be any commercial web site that can facilitate an E-commerce transaction.

Figure 5A is a flow diagram of executable process steps to register a user under the present invention.

The registration process starts in step S5O1.

In step S502, a user enters user specific information. Various fields may be used to develop and store user profiles. A user interface is provided to a user on a display device similar to display device 11. The user may be asked to enter first name, last name, middle initials, electronic mail ("email") address, user name, password, telephone number either land or mobile, pager number, fax number, user address, occupation, and a question that gives a user a hint to remember the user password etc. It is noteworthy that

the present invention is not limited to a particular number of fields for creating user profiles. User profile information is sent to registry 402 in an encrypted form using Secure Socket Layer (SSL) technology. SSL is a 40/128 bit encryption process in the TCP/IP layer of web browsers, such as Netscape ™ and Internet Explorer ™, Profile information is stored in database 403B. Every user chooses a unique username and a password. It is noteworthy that a user can update user profile information subsequently.

In step S503, registry 402 sends an acknowledgement to the user that profile information has been received. Receiving module 403A receives input user information and sends an email or facsimile to the user acknowledging that user information has been received. Receiving module 403A may also send the acknowledgement via a pager etc.

In step S504, a validation process verifies user information sent in step S5Ol. Various levels of security may be used for validation. A level 1 validation may request an acknowledgement from the user after step S503 via electronic mail, facsimile or a telephone call. A level 2 validation may require a user to provide documentary evidence to establish user identity, for example, a copy of a driver's license, social security number, passport, or birth

certificate etc. A level 3 validation, may require a user to personally visit a specific authorization agent, for example, a notary or a service that can provide authorization services for validating and verifying user identity.

After user information is validated in step S504, in step S505, registry 402 places a telephone call to the user. Such telephone calls may be placed to the users cellular or mobile phone or a land phone. Registry 402 uses IVR 403B to place the telephone call. The telephone call is placed to the latest telephone number provided by the user.

In step 506, IVR 403C provides a list of options to the user and prompts the user to select a mobile digital authentication code ("MDC")on a designated device. MDC is a user specific code. MDC is used to authenticate any future E-commerce transaction that may be requested by the user. MDC may be a combination of numeric, alpha numeric or special characters.

In step S507, the user enters the MDC on a designated device. The user previously enters information regarding such designated device, for example cell phone telephone number etc., in step S502. The designated device may be a cell or mobile phone.

The invention is not limited to a cell or mobile phone. A regular land telephone system may be used to enter the MDC. Also other devices may be used to enter the MDC. For example, a two-way pager may be used to enter the MDC. A smart card may also be used to enter the MDC. The Smart Card Industry Association (accessible via the Internet at www.scia.org) provides a description of Smart card technology. One such description is provided in "Smart Cards " by Carol H. Fancher and is incorporated herein by reference, available at www.scia.org/knowledgebase/default.htm.

IVR 403C may also ask the user to confirm MDC more than once after the user has entered the MDC for the first time.

In step S508, MDC is transferred from the designated device to registry 402. MDC may be encrypted at the designated device before being transferred to registry 402. Various encryption techniques may be used to encrypt the MDC before being transferred to registry 402. Receiving module 403A receives the MDC and links the MDC to user identification number. Thereafter the MDC is stored in an encrypted format in database 403E. Various encryption techniques may be used to encrypt MDC code and store the encrypted code at servers 304 and/or 305 as content 306 and/or 307.

Figure 5B is a process flow diagram showing process steps for registering service point 404 such that a user may utilize the authentication/authorization system according to the present invention, while conducting E-commerce transactions.

In step S500A, service point 404 representative logs on to registry 402.

In step S500B, via service point 404, a service point representative enters service point 402 information. Such information may include, name of the service point, address, telephone number, registration number, service point identification number, password and encrypting technique that the service point intends to use.

In step 500C, registry 402 sends an email acknowledging receipt of the registration information. The foregoing process registers a particular service point 404 to use the secured E-commerce transaction system of the present invention.

Figure 6 is a process flow diagram describing the authorization/authentication of an E-commerce transaction, according to the present invention.

In step S601, a user logs onto the website of service point 404(e.g., Amazon.com, a Registered Trademark). The user may use a computing system 10 to log on to service point 404. Service point 404 is previously registered with registry 402 of the present invention (Fig SB). The user sends a request to service point 404 to buy goods and/or services. The user transaction request is received by service point 404. User uses a user identification number and a password to initiate the transaction.

In step S602, service point 404 transfers the user request for the transaction to registry 402 and in particular to receiving module 403A.

In step S603, registry 402 identifies the user based upon user identification number and password stored in database 403B. Thereafter, receiving module 403A generates a transaction identification number that is displayed on service point 404's website. The transaction identification number is visible to the user

on display device 11 while the user is conducting the transaction via service point 404's website.

In step S604, IVR 403s contacts a designated device. If the designated device is a telephone, then IVR 4038 triggers a telephone call to a telephone number provided by the user. It is noteworthy that a cell, mobile or land telephone may be used. Also other devices may used for contact between registry 402 and the user. For example, a two-way pager may be used. A smart card may also be used. The Smart Card Industry Association (accessible via the Internet at www.scia.org) provides a description of Smart card technology. One such description is provided in "Smart Cards " by Carol H. Fancher and is incorporated herein by reference, available at www.scia.org/knowledgebase/default.htm.

In step S605, IVR 403C prompts the user to enter user specific MDC along with the transaction identification number as seen on the service point 404's webpage.

In step S606, the user enters the MDC along with the transaction identification number. The user enters the MDC in a designated device. For example, a mobile or cell phone if the call in step S604 is placed to a cell or mobile phone. If the call in step

S604 is placed to a land phone, then the user may enter the MDC via the land phone. As discussed above, other devices may also be used to enter the MDC.

In step S607, the designated device where the MDC is entered, transfers the MDC to registry 402. Again, as described in step S508 (Fig. SA), the MDC before being transferred may be encrypted.

In step S608, registry 402 compares user entered MDC with user specific MDC stored in database 403B. (Figure SA). Registry 402 also verifies the user entered transaction identification number after comparing it with the transaction identification number generated in step S603.

If the numbers in step S608 match, then in step S609, registry 402 authorizes the user requested E-commerce transaction request. The authorization data is stored in database 403B. Authorization data includes transaction number, date and time of transaction as linked to user identification number, password and MDC. This can assist service point 402 to repudiate any claims by a user that a specific transaction was unauthorized.

One advantage of the present invention is that initiation and authentication of an E-commerce transaction requires two different channels. The main channel provides security for the user to request a transaction and obtain a transaction identification number. The alternate channel assists in authentication. In order to breach the system of the present invention, one will have to know the user login identity and password on the main channel, personal device details, authentication code on the alternate channel, transaction identification number on the main channel and know the algorithm used for encrypting all the data during the transaction. The probability of simultaneously of acquiring the foregoing data is quite remote. Hence the present invention provides a secure system for E-commerce transactions.

Another advantage of the present process is that a user must enter an authentication code for registration via an alternative channel and device, e.g., a cell, mobile or land phone, two-way pager or smart cards etc. Hence even if user password is stolen, the authentication code is still required to proceed with a transaction. This additional channel (authentication code and transaction identification number) provides an extra layer of security for vulnerable E-commerce transactions.

Yet another advantage of the present system is that a user must enter two sets of numbers, one transaction specific, i.e., the transaction identification number, and another user specific, i.e., the authentication code. Since the user must be identified prior to any transaction by entering the authentication code via an alternate channel other than the main E-commerce transaction channel, it provides a degree of security that is much more stringent than identifying the user by merely a password.

Yet another advantage of the present system is that users can authenticate themselves via a mobile phone. Hence the system is flexible.

Yet another advantage of the present invention is that the authentication code is entered on a device (e.g. cell phone or land phone etc.) specified by the user.

Yet another advantage of the present invention is that any transaction authorized by registry is stored for future reference. Hence any claims by the user or a third party against authorized transaction can be repudiated by the stored authorization data.

Microfiche appendix "A" that is attached hereto contain source code in HTML, Java, Java script, Visual basic programming language for programming a computer, are a part of the present disclosure, and are incorporated by reference in their entirety. The attached appendices provide two examples of implementing the foregoing aspects of the present invention. It is noteworthy that the invention is not limited to the examples in the attached appendices, other computer languages may be used to implement the foregoing aspects of the present invention.

Although the present invention has been described with reference to specific embodiments, these embodiments are illustrative only and not limiting. Many other applications and embodiments of the present invention will be apparent in light of this disclosure and the following claims.

CLAIMS

1. A method for authenticating an electronic commerce transaction, comprising: generating a transaction identification number upon receiving a user request for the electronic commerce transaction; contacting a user requesting the electronic commerce transaction; and prompting the user to enter an authentication code for verifying user identity.

2. The method of claim 1, further comprising: prompting the user to enter the transaction identification number.

3. The method of claim 1, further comprising: entering the authentication code, wherein the authentication code is entered via a mobile telephone .

4. The method of claim 2, further comprising: entering the transaction identification number.

5. The method of claim 3, further comprising : comparing the entered authentication code with a previously stored authentication code.

6. The method of claim 4, further comprising: comparing the user entered transaction number to the generated transaction number.

7. A method for registering a user for conducting secured on-line electronic commerce transaction, comprising: entering user profile information; contacting the user whose profile information is entered; and prompting the user to enter an authentication code.

8. The method of claim 7, further comprising: entering the authentication code, wherein the authentication code is entered via a mobile phone; and storing the authentication code with user profile information.

9. A system for authorizing and authenticating electronic commerce transaction, comprising: a registry module that registers users to conduct electronic commerce transactions; and a authentication/authorization module, that initiates a telephone to verify user identity.

10. The system of claim 9, wherein the authorization/ authentication module includes a database for strong user identity data.

11. The system of claim 10, wherein the authorization/ authentication module includes a voice response system that provides a menu of options to users to enter user specific authentication code.

12. The method of Claim 3, wherein the authentication code is entered via a land phone.

13. The method of Claim 3, wherein the authentication code is entered via a two-way pager.

14. The method of Claim 1, wherein the user is contacted via a cell phone.

15. The method of Claim 1, wherein the user is contacted by a land phone.

16. The method of Claim 1, wherein the user is contacted via a two way pager.

17. The method of Claim 7, wherein the user is contacted via a cell phone.

18. The method of Claim 7, wherein the user is contacted by a land phone.

19. The method of Claim 7, wherein the user is contacted via a two way pager.

20. The method of Claim 8, wherein the authentication code is entered via a land phone.

21. The method of Claim 8, wherein the authentication code is entered via a two-way pager.

22. The method of Claim 8, wherein the authentication code is entered via a smart card.

23. The method of Claim 3, wherein the authentication code is entered via a smart card.

APPENDIX "A"

AUTHENTICATION PROCESS FOR HOMETRADE.COM (A WEBSITE FOR E-COMMERCE TRANSACTIONS)

TREE VIEW

```
Files
|___1. www.espacetech.com
|   |
|___2.www. hometrade.htm
        |__displayrandom.jsp
        |
        |__hometrade.jsp
              |
              |___MerLogin.java     ( oyenok.mer.MerLogin)
                  |___MerLogin.class
```

I) HTML FILES

No.	Name	Description (online)	Where to be found
1.	www.espacetech.com	http://www.espacetech.com	online
2.	www.hometrade.com	http://203.197.138.75/hometrade.htm	"

II) GIFs OR JPEGs

No.	Name.	Where to be found
		online

III) JSP FILES

No.	Name.	Where to be found
1.	displayrandom.jsp	\examples\oyenok
2.	hometrade.jsp	

IV) JAVA BEANs(Source files)

No.	Name.	Extention	Where to be found
1.	MerLogin	.java	classes\oyenok\mer\

V) CLASS FILES

No.	Name.	Extionsion	Description	Where to be found
1.	MerLogin.class	.class		classes\oyenok\mer\
2.	Class1	"		classes\oyenok\autnew\
3.	_Class1	"		
4.	JIntegraInit	"		
5.	_Class1Proxy	"		
6.	AuthTest	"		
7.	Test	"		

VI) DLLs

No.	Name.	Extionsion	Description	Where to be found
To be filled.→				

displayrandom.jsp

```
<html>
<head>
<script language="JavaScript">

        function timer() {
        setTimeout("window.status='Closing in 10 seconds'", 1000);
        setTimeout("window.status='Closing in 9 seconds'", 2000);
        setTimeout("window.status='Closing in 8 seconds'", 3000);
        setTimeout("window.status='Closing in 7 seconds'", 4000);
        setTimeout("window.status='Closing in 6 seconds'", 5000);
        setTimeout("window.status='Closing in 5 seconds'", 6000);
        setTimeout("window.status='Closing in 4 seconds'", 7000);
        setTimeout("window.status='Closing in 3 seconds'", 8000);
        setTimeout("window.status='Closing in 2 seconds'", 9000);
        setTimeout("window.status='Closing in 1 seconds'", 10000);
        setTimeout("this.close()",11000);


</script>
</head>
<body onLoad="timer()">
        <center>
        <font face="Arial">Your Transaction ID is
<B><%=request.getParameter("randomval")%></B></font>
        </center>
</body>
<html>
```

---

hometrade.jsp

```
<html>

<head>
<title>OyeNok Auth. V</title>
</head>

<jsp:useBean id="user" scope="page" class="oyenok.mer.MerLogin">
<jsp:setProperty name="user" property="*" />
<% if (!user.callUser()) { %>
```

```
        <body>
        Not a Registered User
<% } else { %>
        <body
onLoad="location.href='http://www.hometrade.com/default.asp?M27PRJ=HomePage&D
ISPATCHER=HTS_HPG_004'">
        <center> You are successfully authorized, you will be taken to hometrade.com
</center>
<% } %>
</jsp:useBean>
</body>
</html>
```

MerLogin.java

```
package oyenok.mer;

import java.sql.

public class MerLogin
        String name;
        String password;
        String random;

        public String getName() {
                return name;
        }
        public void setName(String name) {
                this.name = name;
        }
        public void setPassword(String password) {
                this.password = password;
        }
        public void setRandom(String random) {
                this.random = random;
        }


        public boolean callUser() {
                try {
                        Class.forName("sun.jdbc.odbc.JdbcOdbcDriver");
                        Connection con =
DriverManager.getConnection("jdbc:odbc:oyenokDSN","sa","");
                        Statement st = con.createStatement();
```

```
                    String query = "SELECT creditno from USER_DETAILS
WHERE userid='" + name + "'";

                    ResultSet rs = st.executeQuery(query);
                    rs.next();
                    String ccID = rs.getString(1);

                    oyenok.authenticate.AuthTest obj = new
oyenok.authenticate.AuthTest();
                    obj.setRandom(ccID, random, "");
                    return obj.authenCall(ccID);
                }catch(Exception e) {
                    return false;
                }

                try {
                    Class.forName("sun.jdbc.odbc.JdbcOdbcDriver");
                    Connection con =
DriverManager.getConnection("jdbc:odbc:oyenokDSN","sa","");
                    Statement st = con.createStatement();
                    String query = "SELECT creditno from USER_DETAILS
WHERE userid='" + name + "'";

                    ResultSet rs = st.executeQuery(query);
                    rs.next();
                    String ccID = rs.getString(1);

                    query = "UPDATE USER_DETAILS SET randomno='" + random
+ "' WHERE userid='" + name + "'";
                    st.executeUpdate(query);

                    oyenok.autnew.Class1 obj=null;
                    try {
                        String strArr[] = new String[1];
                        strArr[0] = ccID;
                        com.linar.jintegra.AuthInfo authInfo = new
com.linar.jintegra.AuthInfo("Workgroup", "Administrator", "");
                        obj = new oyenok.autnew.Class1("10.10.1.36", authInfo);
                        return obj.callNumb(strArr);
                    }catch(Exception e) {
                        System.out.println(e);
                        return false;
                    }finally{
                        com.linar.jintegra.Cleaner.release(obj);
                    }
                }catch(Exception e) {
```

```
                System.out.println(e);
                return false;
            }


    }
    public static void main(String ags[]) {
            System.out.println(new MerLogin().callUser());
    }
}
```

authentication.dll

```
Dim WithEvents VoiceBocx1 As VoiceBocx
Dim Flag As Boolean
Dim ivrConn As ADODB.Connection
Dim ivrRs As ADODB.Recordset
Dim temp As Integer

Private Sub Initialize()

Set VoiceBocx1 = New VoiceBocx
Flag = False

VoiceBocx1.Log = LOG_Detailed
Set chConn = CreateObject("ADODB.Connection")
Set chRs = CreateObject("ADODB.Recordset")
chConn.Open "samDSN", "sa", ""

Set VoiceBocx1 = New VoiceBocx

' Set the Logging level to 'Detailed'
VoiceBocx1.Log = LOG_Detailed

' Assign the TrunkChannel from the command line argument (if any)
If Len(Command) > 0 Then
   VoiceBocx1.TrunkChannel = Val(Command)
Else
   ' The default channel is the 1st channel (number zero.)
   VoiceBocx1.TrunkChannel = 0
End If


End Sub
Private Sub Terminate()

 Set VoiceBocx1 = Nothing
 ivrConn.Close
 Set ivrRs = Nothing
```

```
Set ivrConn = Nothing


End Sub

Private Sub HandleOutboundCall()

Dim random, lInput, lNumber As String
Dim ccNo, telno, autId As String
Dim flag1 As Boolean

If VoiceBocx1.HangupIsRuntimeError = True Then
' MsgBox "Caller HungUP"
flag1 = False
Flag = False
End If

If flag1 = False Then
 'MsgBox ("Playing Welcome Message.")
VoiceBocx1.PlayFile ("C:\messages\welcome7.vox")


VoiceBocx1.PlayFile ("C:\messages\transId.vox")
lInput = VoiceBocx1.GetDigits(13, 20, 15, "#")
Dim Length
Length = Len(lInput)
Length = Length - 1
lInput = Mid(lInput, 1, Length)

Dim temp1
temp1 = ivrRs.Fields(7) & ivrRs.Fields(10)

If lInput = Val(temp1) Then
 VoiceBocx1.PlayFile ("C:\messages\thanks0.vox")
 'MsgBox "The User is Authenticated"
 Flag = True
 Else
  MsgBox "The user is Invalid"
  VoiceBocx1.PlayFile ("C:\messages\notautherror.vox")
  Flag = False
 End If

 ErrorTrap:
    ' If it is a hangup, exit normally
    If VoiceBocx1.TrunkStateName = "RemoteDisconnected" Then
      ' MsgBox ("Caller hung up.")
       Call VoiceBocx1.DisconnectCall
       Call Terminate
    End If

 End If
 End Sub
```

```
Set ivrConn = CreateObject("ADODB.Connection")
Set ivrRs = CreateObject("ADODB.Recordset")
ivrConn.Open "chDSN", "sa", ""

'MsgBox "Inside Testing Again"
Call Initialize

sql = "Select *  from user_details where credino =" & _
"'" & ccNum & "'"
```

```
ivrRs.Open sql, ivrConn, adOpenDynamic, adLockOptimistic

phoneNumber$ = ivrRs.Fields(4)

Call VoiceBocx1.MakeCall(phoneNumber$, True)

Select Case (VoiceBocx1:TrunkStateName)
 Case "Connected"
    If (VoiceBocx1.GlareDetected) Then
        ' MsgBox "Glare - Connected Inbound"
         Call VoiceBocx1.DisconnectCall
         Call Terminate
    End If

  ' MsgBox "Connected Outbound"
    Call HandleOutboundCall

 Case "NoConnect"
  ' MsgBox "NoConnect"
End Select
ivrRs.Close

Call Terminate
DialNumb = Flag

End Function
```

APPENDIX "B"

AUTHENTICATION PROCESS FOR BUYBOOK.COM (A WEBSITE FOR E-COMMERCE TRANSACTIONS)

TREE VIEW

Files
- 1. buybook.htm
  - 1. displayrandom.jsp
  - 2. authenticate.jsp
    - 1. Eventupdate.class.+ Eventupdate.java (oyenok.authenticate.Eventupdate)

I) HTML FILES

No.	Name	Description	Where to be found
1.	buybook.htm	The stimulated Buy Book Site	\examples\oyenok\

II) GIFs OR JPEGs

No.	Name.	Where to be found
1	certified.gif	examples\oyenok\images\
2	wpe2.gif	"
3.	wpe3.gif	"
4	icon-vhs.gif	"
5	sbutton-save-for-later.gif	"
6	sbutton-delete.gif	"
7	icon-books.gif	"
8	sbutton-save-for-later.gif	"
9	sbutton-delete.gif	"
10	icon-vhs.gif	"
11	sbutton-save-for-later.gif	"
12	sbutton-delete.gif	"
13	wpe4.gif	"
14	tokila.gif	"
15	0130893404.01.MZZZZZZZ.jpg	"
16	1861003625.01.MZZZZZZZ.jpg	"

III) JSP FILES

No.	Name.	Where to be placed
1.	displayrandom.jsp	\examples\oyenok\
2.	authenticate.jsp	\examples\oyenok\

IV) JAVA BEANs(Source files)

No.	Name.	Extension	Description	Where to be placed
1.	Eventupdate	.java		\classes\oyenok\authenticate\

V) CLASS FILES

No.	Name.	Extension	Description	Where to be placed
1.	Eventupdate	.class		\classes\oyenok\authenticate\

VI) DLLs

No.	Name.	Extionsion	Description	Where to be placed

To be filled→

Buybook.htm

```
<html>

<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>ABC Book Stall</title>

<script language="javascript">
function creditcheck()
{

}
</script>

</head>

<body>

<table width="91%" border="0" cellpadding="0" cellspacing="0" height="576">
 <tr>
  <td width="17%" rowspan="2" valign="top" align="left" bgcolor="#FFCC99"
height="576">
   <table width="100%" border="0" cellpadding="0" height="467">
    <tr>
     <td width="100%" height="140" valign="top" align="left"><img border="0"
src="certified.gif" align="right" width="136" height="134"></td>
    </tr>
    <tr>
     <td width="100%" height="21"></td>
    </tr>
    <tr>
     <td width="100%" height="33">
      <table width="100%" border="0" cellpadding="0" cellspacing="0">
       <tr>
        <td width="13%"></td>
        <td width="77%" bgcolor="#C0C0C0" bordercolor="#000000">
        <p align="center">Home
        </td>
        <td width="10%"></td>
       </tr>
      </table>
     </td>
    </tr>
```

```
<tr>
 <td width="100%" height="33">
  <table width="100%" border="0" cellpadding="0" cellspacing="0">
   <tr>
    <td width="12%"> </td>
    <td width="78%" bgcolor="#C0C0C0"
     <p align="center">Library
    </td>
    <td width="10%"> </td>
   </tr>
  </table>
 </td>
</tr>
<tr>
 <td width="100%" height="33">
  <table width="101%" border="0" cellpadding="0" cellspacing="0">
   <tr>
    <td width="12%"> </td>
    <td width="76%" bgcolor="#C0C0C0">
     <p align="center">Research
    </td>
    <td width="13%"> </td>
   </tr>
  </table>
 </td>
</tr>
<tr>
 <td width="100%" height="33">
  <table width="100%" border="0" cellpadding="0" cellspacing="0">
   <tr>
    <td width="12%"> </td>
    <td width="77%" bgcolor="#C0C0C0">
     <p align="center">Online Notes
    </td>
    <td width="11%"> </td>
   </tr>
  </table>
 </td>
</tr>
<tr>
 <td width="100%" height="33">
  <table width="100%" border="0" cellpadding="0" cellspacing="0">
   <tr>
    <td width="13%"> </td>
    <td width="76%" bgcolor="#C0C0C0">
     <p align="center">Security
```

```
            </td>
            <td width="11%"></td>
           </tr>
          </table>
         </td>
        </tr>
        <tr>
         <td width="100%" height="33">
          <table width="100%" border="0" cellpadding="0" cellspacing="0">
           <tr>
            <td width="13%"> </td>
            <td width="76%" bgcolor="#C0C0C0">
             <p align="center">Author's Notes
            </td>
            <td width="11%"> </td>
           </tr>
          </table>
         </td>
        </tr>
        <tr>
         <td width="100%" height="21"> </td>
        </tr>
        <tr>
         <td width="100%" height="21"> </td>
        </tr>
        <tr>
         <td width="100%" height="21"> </td>
        </tr>
        <tr>
         <td width="100%" height="21"> </td>
        </tr>
        <tr>
         <td width="100%" height="21"></td>
        </tr>
        <tr>
         <td width="100%" height="21"></td>
        </tr>
       </table>
      </td>
      <td width="83%" valign="top" align="left" height="540">
       <table width="99%" border="0" cellpadding="0" cellspacing="0" height="463">
        <tr>
         <td width="64%" height="58" valign="baseline" align="center"><img border="0"
src="wpe2.gif" width="368" height="43" align="left"><img border="0" src="wpe3.gif"
width="233" height="43" align="right"></td>
         <td width="36%" height="58" valign="top" align="left"></td>
```

```
        </tr>
        <tr>
         <td width="64%" height="442">
          <table border="0" width="231" cellspacing="0" cellpadding="0" height="167">
           <tr>
 <td width="24"> </td>
 <td width="247"><font face=verdana,arial,helvetica size=-1><b>Shopping Cart Items--
 To Buy Now</b></font></td>
 <td width="26">

 <div align="center"><font face=verdana,arial,helvetica size=-1>Qty.</font></div>

 </td>
 <td width="52"> </td>
 <td width="161"> </td>
           </tr>
           <tr>
 <td width="24" valign="TOP">
   <img alt="Icon" border="0" src="images/icon-vhs.gif" width="22" height="22">
 </td>
 <td bgcolor="#FFFFFF" width="247">
 <a href="/exec/obidos/ASIN/B00000K02F/104-7652825-2097546"><em>Prenatal Yoga
 with Colette Crawford</em></a>

 <br>

 <b>VHS</b>

 <br>

 Usually ships in 24 hours<BR>
     </td>

    <td align=center bgcolor="#FFFFFF" width="26">

       <input type="text" name=quantity.B00000K02F size=4 maxlength=4 value=1
 >edit>

    </td>

    <td width="52" bgcolor="#FFFFFF">

 <font size=2 face=verdana,arial,helvetica color=#000000>

    <NOBR><b>Our Price: <font color=#990000>$24.95</font></b></NOBR><br>
```

```
</font>
    </td>
    <td align=right width="161">

    <input border="0" name="submit.move-to-save.B00000K02F" src="images/sbutton-
save-for-later.gif" type="image" value="Save item" width="70" height="14">
<p>
    <input align="right" border="0" name="submit.delete.B00000K02F"
src="images/sbutton-delete.gif" type="image" value="Delete item" width="42"
height="16">

    </td>
        </tr>
        <tr>
          <td colspan=5 width="467">
</td>
        </tr>
        <tr>
<td width="24" valign="TOP">
    <img alt="Icon" border="0" src="images/icon-books.gif" width="22" height="22">
</td>
<td bgcolor="#FFFFFF" width="247">
<a href="/exec/obidos/ASIN/0130893404/104-7652825-2097546"><em>Core Servlets
and JavaServer Pages (JSP)</em></a>

<br>

Marty Hall;

<b>Paperback</b>

<br>

Usually ships in 24 hours<BR>
     </td>

    <td align=center bgcolor="#FFFFFF" width="26">

<input type="text" name=quantity.0130893404 size=4 maxlength=4 value=1>

    </td>

    <td width="52" bgcolor="#FFFFFF">

<font size=2 face=verdana,arial,helvetica color=#000000>
```

```
    <NOBR>List Price: <strike>$42.99</strike></NOBR><br>

    <NOBR><b>Our Price: <font color=#990000>$34.39</font></b></NOBR><br>

   <NOBR>You Save: <font color=#990000>$8.60 (20%)</font></NOBR>


</font>
    </td>

    <td align=right width="161">

    <input border="0" name="submit.move-to-save.B00000K02F" src="images/sbutton-
save-for-later.gif" type="image" value="Save item" width="70" height="14">
<p>
    <input align="right" border="0" name="submit.delete.B00000K02F"
src="images/sbutton-delete.gif" type="image" value="Delete item" width="42"
height="16">

    </td>
        </tr>
        <tr>
         <td colspan=5 width="467">
</td>
        </tr>
        <tr>
<td width="24" valign="TOP">
       <img border=0  width=22 height=22 src=images/icon-vhs.gif alt=Icon>
</td>
<td bgcolor="#FFFFFF" width="247">
<a href="/exec/obidos/ASIN/0783222955/104-7652825-2097546"><em>To Kill a
Mockingbird</em></a>

(1969)

<br>

Gregory Peck;

<b>VHS</b>; Widescreen

<br>

Usually ships in 24 hours<BR>
    </td>
```

```
    <td align=center bgcolor="#FFFFFF" width="26">
<input type="text" name=quantity.0783222955 size=4 maxlength=4 value=1>
    </td>
    <td width="52" bgcolor="#FFFFFF">
```

```
<font size=2 face=verdana,arial,helvetica color=#000000>

    <NOBR>List Price: <strike>$19.98</strike></NOBR><br>
    <NOBR><b>Our Price: <font color=#990000>$13.99</font></b></NOBR><br>
   <NOBR>You Save: <font color=#990000>$5.99 (30%)</font></NOBR>
</font>
    </td>
    <td align=right width="161">
    <input border="0" name="submit.move-to-save.B00000K02F" src="images/sbutton-
save-for-later.gif" type="image" value="Save item" width="70" height="14">
<p>
    <input align="right" border="0" name="submit.delete.B00000K02F"
src="images/sbutton-delete.gif" type="image" value="Delete item" width="42"
height="16">

    </td>
        </tr>
        <tr>
          <td colspan=5 width="467">
</td>
        </tr>
        <tr>
<td align=right colspan=2 valign=middle width="273">
If you changed any quantities, please start again.
</td>
<td valign=middle width="26">

</td>
```

```
<td colspan=2 width="215">
<font face=verdana,arial,helvetica size=-1><b>Subtotal: <font
color=#990000>$73.33  </font></b><p>
</font>
 

</td>

          </tr>
         <tr>
<td align=right colspan=5 valign=middle width="513">
<table cellspacing="2" cellpadding="4" border="0" width="707">
  <tr>
   <td colspan="2" bgcolor="#EEEECC" width="175"><b><font
face="verdana,arial,helvetica" size="1">Payment
    Method</font></b></td>
   <td bgcolor="#EEEECC" width="221"><b><font face="verdana,arial,helvetica"
size="1">Credit
    Card No.</font></b></td>
   <td bgcolor="#EEEECC" nowrap width="197"><font size="1"> <b><font
face="verdana,arial,helvetica">Expiration
    Date</font></b> </font></td>
   <td bgcolor="#EEEECC" nowrap width="156"><font size="1"> <b><font
face="verdana,arial,helvetica">Cardholder's
    Name</font></b> </font></td>
  </tr>
  <form name="transact" method="post" action="">
  <tr>
   <td width="18"><input type="radio" value="new-card" name="payment-method"
checked></td>
   <td width="145"><select name="issuer">
     <option value="V">Visa
     <option value="M">MasterCard
     <option value="A">American Express
     <option value="I">Diners Club
     <option value="D">Discover
     <option value="J">JCB
    </select></td>
   <td width="221"><input type="text" size="3" name="card1" onblur="creditcheck()">-
<input type="text" size="3" name="card2" onblur="creditcheck()">-<input type="text"
size="3" name="card3" onblur="creditcheck()">-<input type="text" size="3"
name="card4" onblur="creditcheck()"></td>
   <td width="197"><nobr><select name="cc-exp-month">
     <option value="01">01
     <option value="02">02
     <option value="03">03
```

```
        <option value="04">04
        <option value="05">05
        <option value="06">06
        <option value="07">07
        <option value="08">08
        <option value="09">09
        <option value="10">10
        <option value="11">11
        <option value="12">12
      </select><select name="cc-exp-year">
        <option value="2000">2000
        <option value="2001">2001
        <option value="2002">2002
        <option value="2003">2003
        <option value="2004">2004
        <option value="2005">2005
        <option value="2006">2006
        <option value="2007">2007
        <option value="2008">2008
        <option value="2009">2009
        <option value="2010">2010
        <option value="2011">2011
        <option value="2012">2012
        <option value="2013">2013
        <option value="2014">2014
        <option value="2015">2015
        <option value="2016">2016
        <option value="2017">2017
        <option value="2018">2018
      </select></nobr></td>
    <td width="156"><input type="text" size="20" value name="cardholder-name"></td>
    <tr>
      <td width="18"></td>
      <td width="145">Enter OyeNok ID (If already registered)</td>
      <td width="221"><input type="text" size="20" name="card-number"></td>
      <td width="197"><p align="center"><a href="authenticate.htm"><font
face="Bookman Old Style" size="2">Submit</font></a></td>
    <td width="156">
      <nobr>If not  Registered</nobr> <a href="signup.htm">Click
      here</a></td>
    <tr>
      <td width="18" valign="top"><input type="radio" value="check" name="payment-
method"></td>
      <td valign="top" colspan="4" width="658"><font face="verdana,arial,helvetica"
size="-1">Pay
```

```
        by check or money order</font>  <font face="verdana,arial,helvetica"
 size="-2">(or check funds on
        account)</font></td>
      </tr>
    </table>
        </td>
    </tr>
     </form>

    </table>
       </td>
       <td width="36%" height="442" valign="top" align="left">
         
        <table border="0" width="100%" cellspacing="0" cellpadding="0"
height="458">
          <tr>
           <td width="5%" height="458" valign="top" align="left">
            <table border="0" width="1%" bgcolor="#9A9CB4" cellspacing="0"
cellpadding="0">
              <tr>
               <td width="100%"> 
                <p> </p> <p> </p> <p> </p> <p> </p>
<p> </p> <p> </p> <p> </p>
                <p> </p> <p> </p> <p> </p> <p> </p>
<p> </p> <p> </p>
               </td>
              </tr>
             </table>
           </td>
           <td width="95%" valign="top" align="left" height="458">
           <img border="0" src="images/wpe4.gif" width="95" height="62"><img
align="left" border="1" hspace="5" src="images/tokila.gif" vspace="3" width="76"
height="140">
           <p> </p> <p> </p> <p> </p> <p> </p>
           <p><img align="left" border="1" hspace="5"
src="http://images.amazon.com/images/P/0130893404.01.MZZZZZZZ.jpg" vspace="3"
width="105" height="140"></p>
           <p> </p> <p> </p>          <p> </p>
           <p> </p>
           <p><img align="left" border="1" hspace="5"
src="http://images.amazon.com/images/P/1861003625.01.MZZZZZZZ.jpg" vspace="3"
width="111" height="140">
           </p>
           <p> </p>
           <p> </p>
           <p> </p>
```

```
            <p> 
            </td>
           </tr>
          </table>
         </td>
        </tr>
        <tr>
         <td width="64%" height="1" valign="top" align="left">
         </td>
         <td width="36%" height="1" valign="top" align="left">
              &nbs
          p;           
;     
        </td>
       </tr>
      </table>
     </td>
    </tr>
    <tr>
     <td width="83%" valign="baseline" align="left" height="36">
      <p align="center"><font face="Garamond" size="3">Home | Library |
      Research | Online notes | Security | Author's notes</font></p>
     </td>
    </tr>
</table>

</body>

</html>
```

---

authenticate.jsp

```
<html>
<body>
        <jsp:useBean id="authenid" scope="page" class="oyenok.aut.AuthTest">
                <% authenid.setRandom(request.getParameter("creditcardno"),
request.getParameter("randomval")); %>
                <% if ( authenid.authenCall(request.getParameter("creditcardno")) ) {%>
                        You are Successfully Authenticated
                <% } else { %>
                        Sorry, the Authentication failed
                <% } %>
        </jsp:useBean>
</body>
</html>
```

displayrandom.jsp

```
<html>
<head>
<script language="JavaScript">

        function timer() {
        setTimeout("window.status='Closing in 10 seconds'", 1000);
        setTimeout("window.status='Closing in 9 seconds'", 2000);
        setTimeout("window.status='Closing in 8 seconds'", 3000);
        setTimeout("window.status='Closing in 7 seconds'", 4000);
        setTimeout("window.status='Closing in 6 seconds'", 5000);
        setTimeout("window.status='Closing in 5 seconds'", 6000);
        setTimeout("window.status='Closing in 4 seconds'", 7000);
        setTimeout("window.status='Closing in 3 seconds'", 8000);
        setTimeout("window.status='Closing in 2 seconds'", 9000);
        setTimeout("window.status='Closing in 1 seconds'", 10000);
        setTimeout("this.close()",11000);
        }

</script>
</head>
<body onLoad="timer()">
        <center>
        Your Transaction ID is <%=request.getParameter("randomval")%>
        </center>
</body>
<html>
```

Eventupdate.java

```
package rangoyenok.authenticate;

import java.io.*;
import java.util.*;
import java.sql.*;

public class Eventupdate {

        String eventid,event,process,userid,time,status,servertime;

        public Eventupdate(){}
```

```
public void setEventid(String eventid) {
this.eventid = eventid;
}

public void setEvent(String event) {
this.event = event;
}

public void setProcess(String process) {
this.process = event;
}

public void setUserid(String userid) {
this.userid = userid;
}

public void setTime(String time) {
this.time = time;
}

public void setStatus(String status) {
this.status = status;
}

public void setServertime(String servertime) {
this.servertime = servertime;
}

public boolean setEvents() {

try {

        Class.forName("sun.jdbc.odbc.JdbcOdbcDriver");
        Connection con =
DriverManager.getConnection("jdbc:odbc:OyenokDSN","sa","");
        Statement st = con.createStatement();

        String query = "INSERT INTO oyenok_events
values("+"'"+eventid+"','"+event+"','"+process+"','"+userid+"','"+time+"','"+status+"','"+s
ervertime+"')";

        st.executeUpdate(query);

  }catch(Exception e) { System.out.println(e); }
     return true;
}
```

```
        public static void main(String s[]){
        Eventupdate objeventupdate =  new Eventupdate();
                try {
objeventupdate.setEvents("event3","cc_sent_for_validation","Proc2","user2","7:48:00","
1","12/12/99");
                        } catch(Exception e) {System.out.println(e);}
 } */

}

//String eventid, String event, String process, String userid,String time, String status,
//String servertime
```

---

authentication.dll

```
Dim WithEvents VoiceBocx1 As VoiceBocx
Dim Flag As Boolean
Dim ivrConn As ADODB.Connection
Dim ivrRs As ADODB.Recordset
Dim temp As Integer

Private Sub Initialize()

Set VoiceBocx1 = New VoiceBocx
Flag = False

VoiceBocx1.Log = LOG_Detailed
Set chConn = CreateObject("ADODB.Connection")
Set chRs = CreateObject("ADODB.Recordset")
chConn.Open "samDSN", "sa", ""

Set VoiceBocx1 = New VoiceBocx

' Set the Logging level to 'Detailed'
VoiceBocx1.Log = LOG_Detailed

' Assign the TrunkChannel from the command line argument (if any)
If Len(Command) > 0 Then
   VoiceBocx1.TrunkChannel = Val(Command)
Else
   ' The default channel is the 1st channel (number zero.)
   VoiceBocx1.TrunkChannel = 0
End If


End Sub
```

```
Private Sub Terminate()
 Set VoiceBocx1 = Nothing
 ivrConn.Close
 Set ivrRs = Nothing
 Set ivrConn = Nothing
End Sub

Private Sub HandleOutboundCall()
Dim random, lInput, lNumber As String
Dim ccNo, telno, autId As String
Dim flag1 As Boolean
If VoiceBocx1.HangupIsRuntimeError = True Then
' MsgBox "Caller HungUP"
flag1 = False
Flag = False
End If
If flag1 = False Then
 MsgBox ("Playing Welcome Message.")
VoiceBocx1.PlayFile ("C:\messages\welcome7.vox")
 VoiceBocx1.PlayFile ("C:\messages\transId.vox")
 lInput = VoiceBocx1.GetDigits(13, 20, 15, "#")
 Dim Length
 Length = Len(lInput)
 Length = Length - 1
 lInput = Mid(lInput, 1, Length)
 Dim temp1
 temp1 = ivrRs.Fields(7) & ivrRs.Fields(10)
 If lInput = Val(temp1) Then
  VoiceBocx1.PlayFile ("C:\messages\thanks0.vox")
  MsgBox "The User is Authenticated"
  Flag = True
  Else
   MsgBox "The user is Invalid"
   VoiceBocx1.PlayFile ("C:\messages\notautherror.vox")
   Flag = False
 End If

ErrorTrap:
   ' If it is a hangup, exit normally
   If VoiceBocx1.TrunkStateName = "RemoteDisconnected" Then
     ' MsgBox ("Caller hung up.")
      Call VoiceBocx1.DisconnectCall
      Call Terminate
   End If
```

```
End If
End Sub


Public Function DialNumb(ccNum As String) As Boolean

Set ivrConn = CreateObject("ADODB.Connection")
Set ivrRs = CreateObject("ADODB.Recordset")
ivrConn.Open "chDSN", "sa", ""

'MsgBox "Inside Testing Again"
Call Initialize

sql = "Select * from user_details where creditno =" & _
"'" & ccNum & "'"

ivrRs.Open sql, ivrConn, adOpenDynamic, adLockOptimistic

phoneNumber$ = ivrRs.Fields(4)

Call VoiceBocx1.MakeCall(phoneNumber$, True)

Select Case (VoiceBocx1.TrunkStateName)
Case "Connected"
   If (VoiceBocx1.GlareDetected) Then
         MsgBox "Glare - Connected Inbound"
         Call VoiceBocx1.DisconnectCall
         Call Terminate
   End If

   MsgBox "Connected Outbound"
   Call HandleOutboundCall

Case "NoConnect"
   MsgBox "NoConnect"
End Select
ivrRs.Close

Call Terminate
DialNumb = Flag

End Function
```

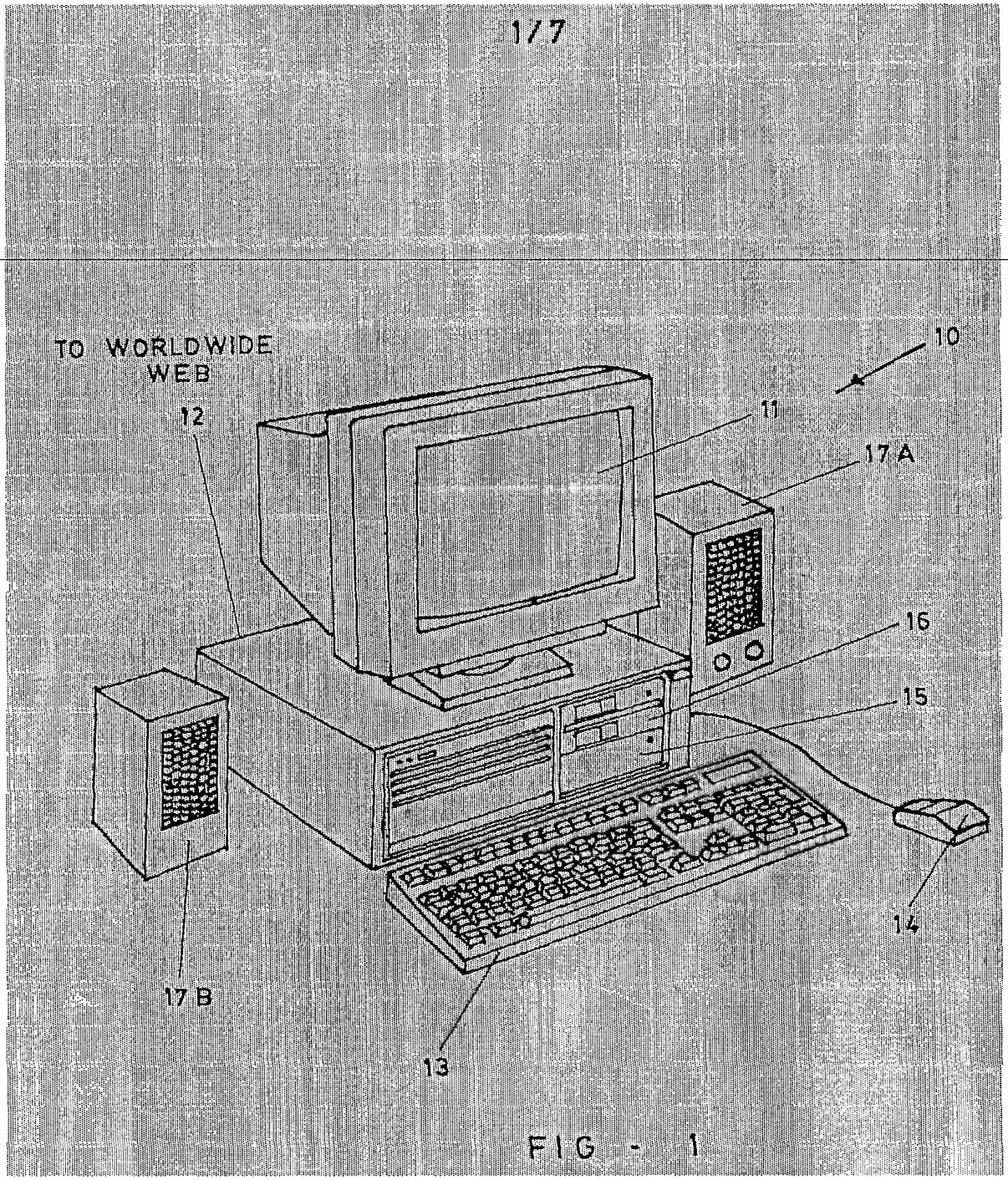


FIG - 1

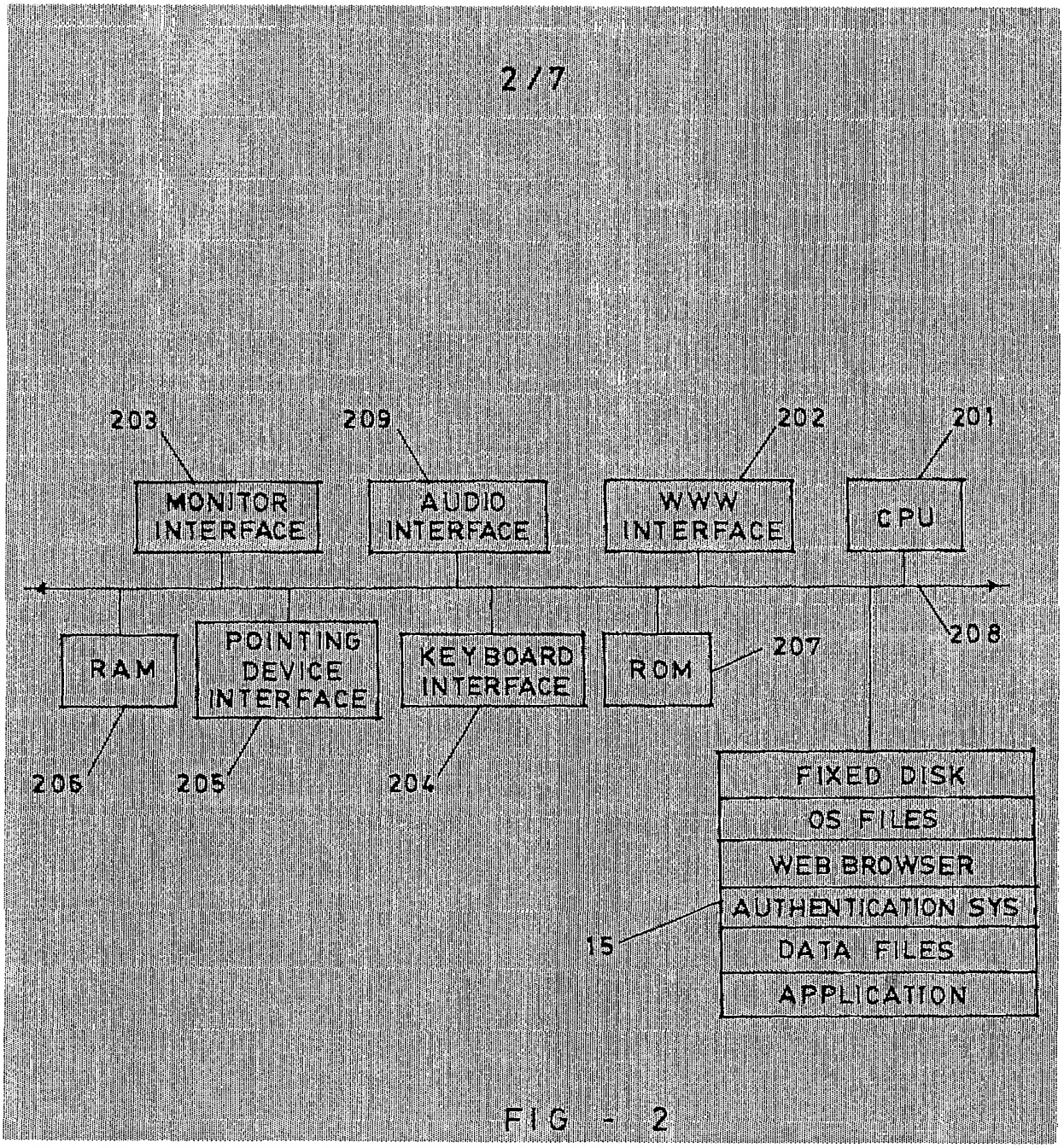


FIG - 2

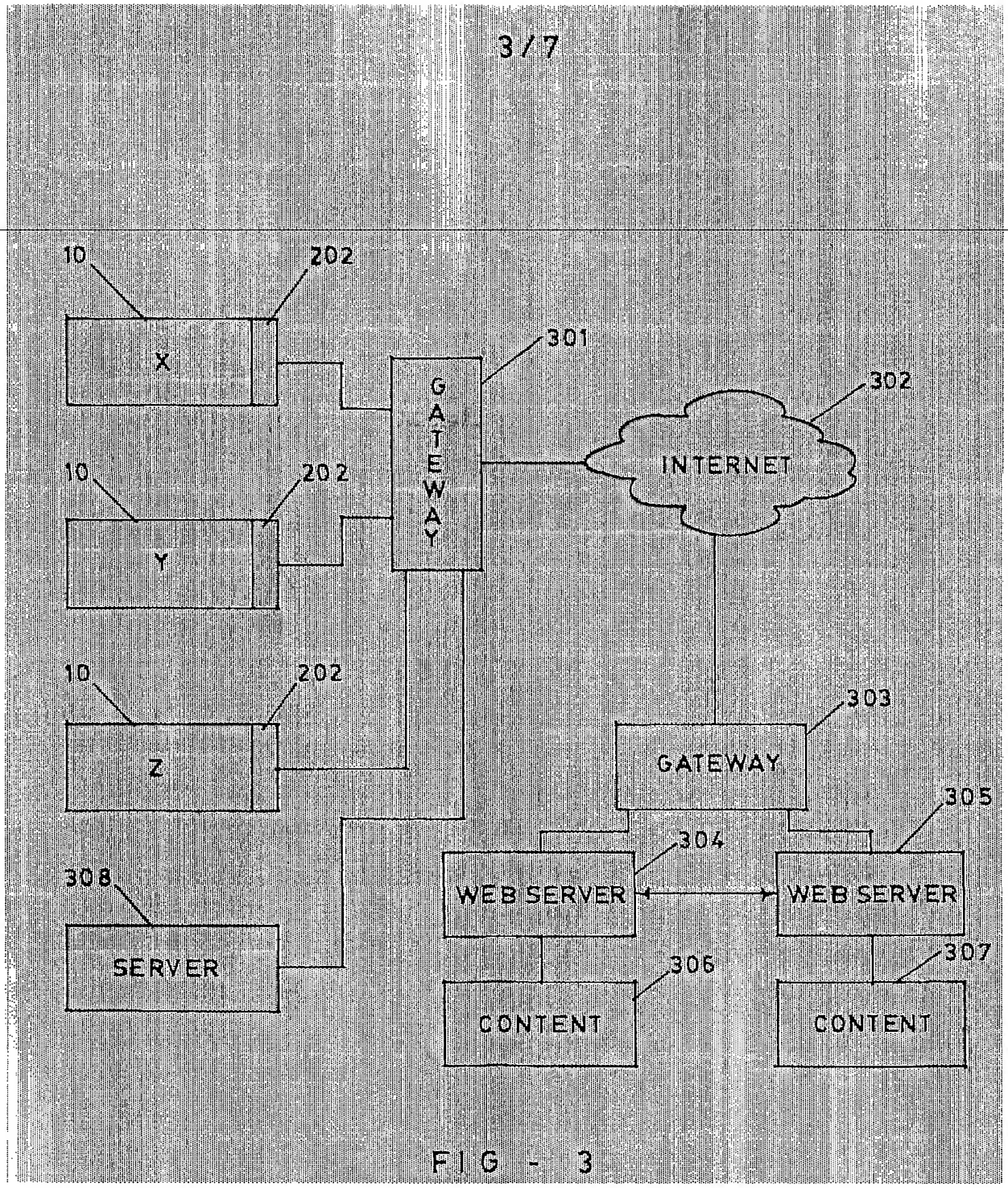


FIG - 3

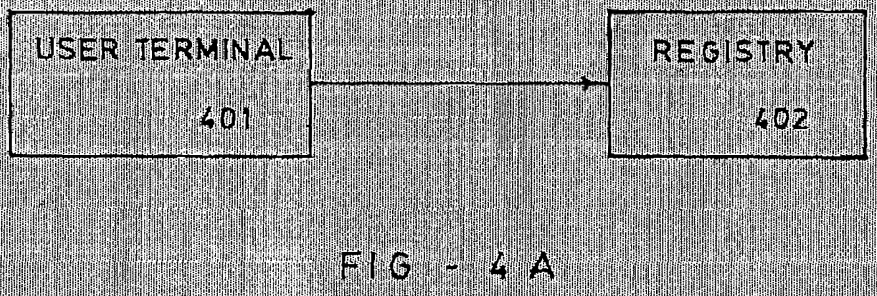
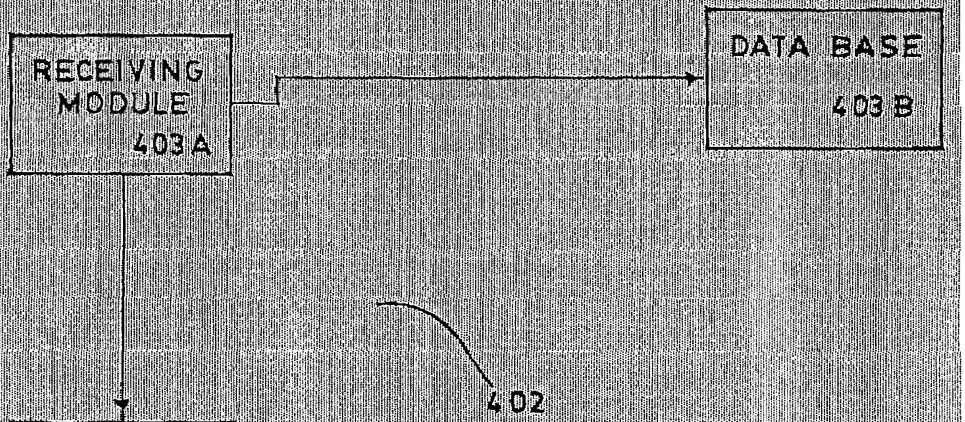
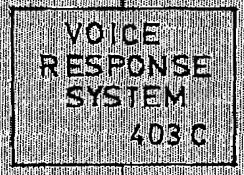


FIG - 4A





TO MOBILE CHANNEL
403D

FIG - 4B

FIG - 4C

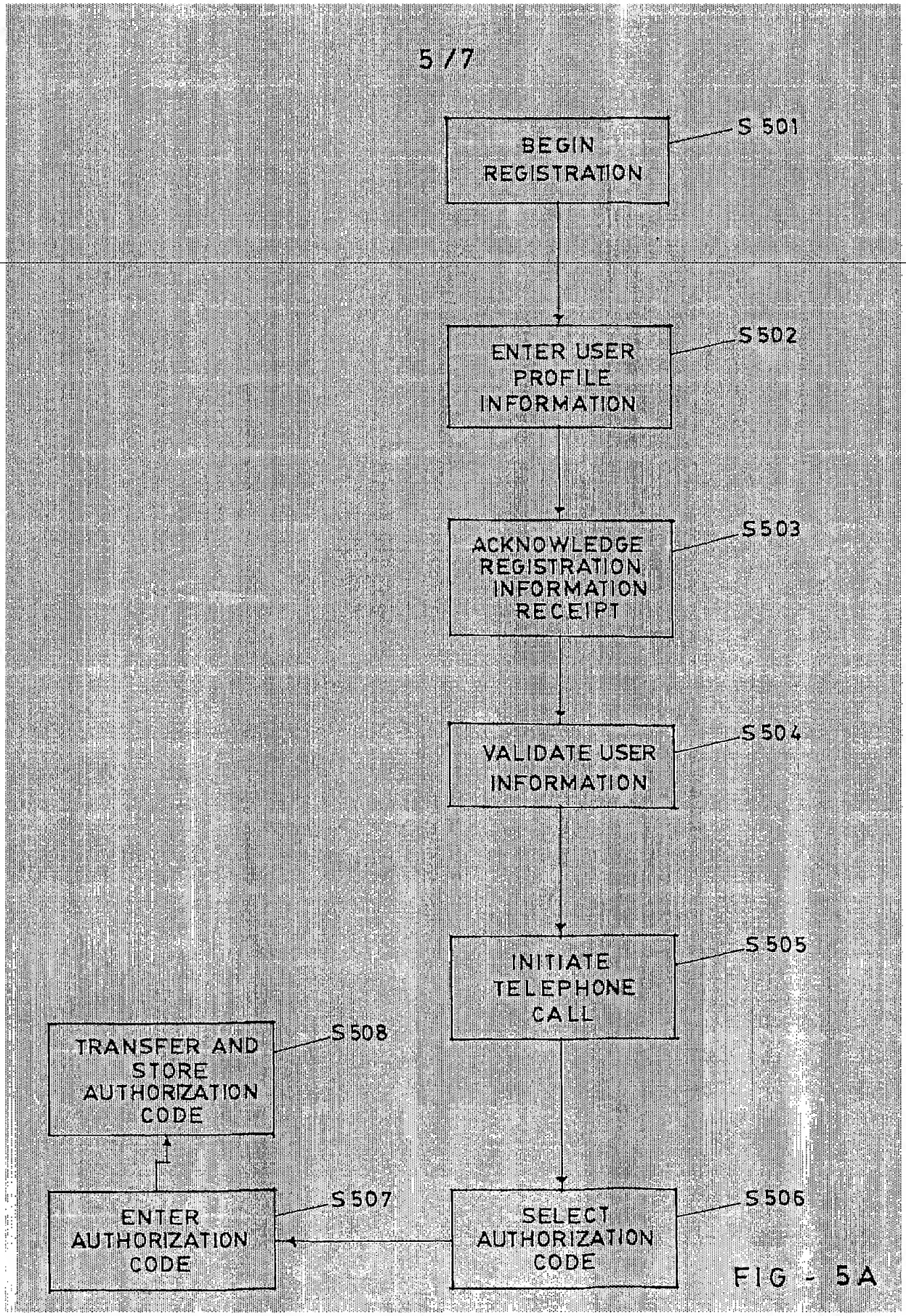


FIG - 5A

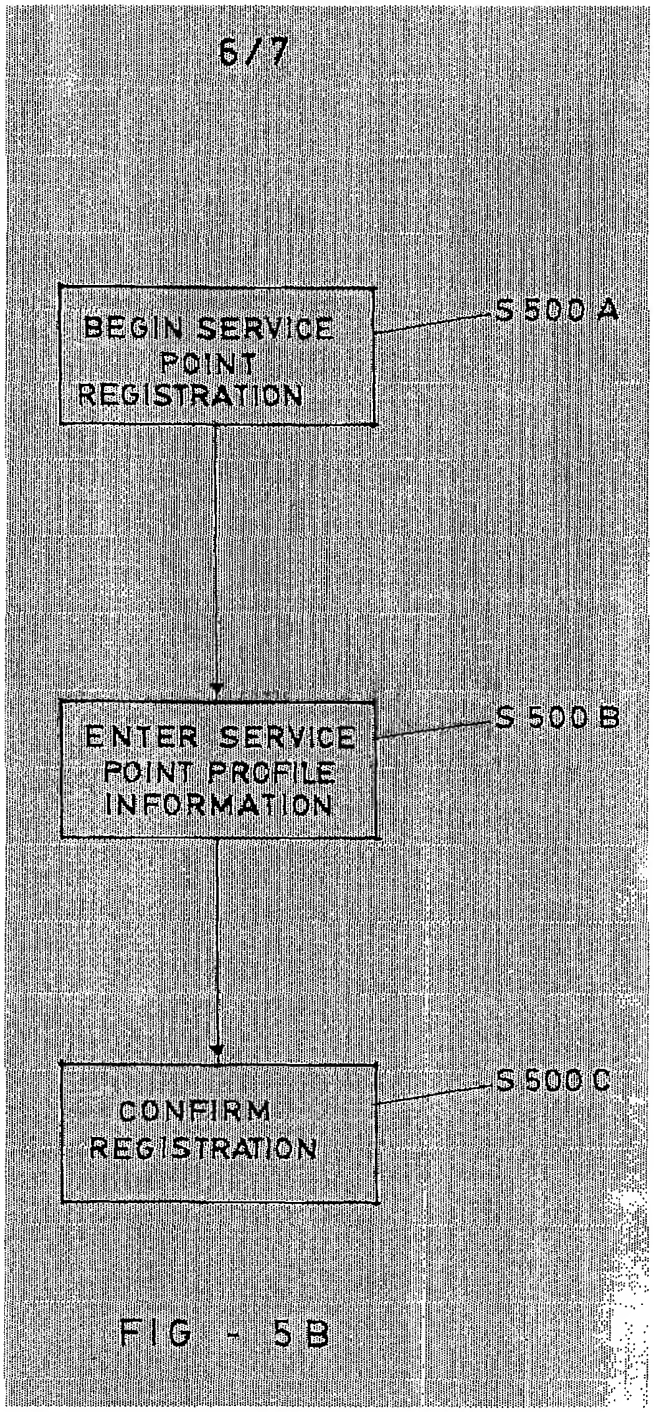

BEGIN SERVICE POINT REGISTRATION
S 500 A
ENTER SERVICE POINT PROFILE INFORMATION
S 500 B
CONFIRM REGISTRATION
S 500 C

FIG - 5B

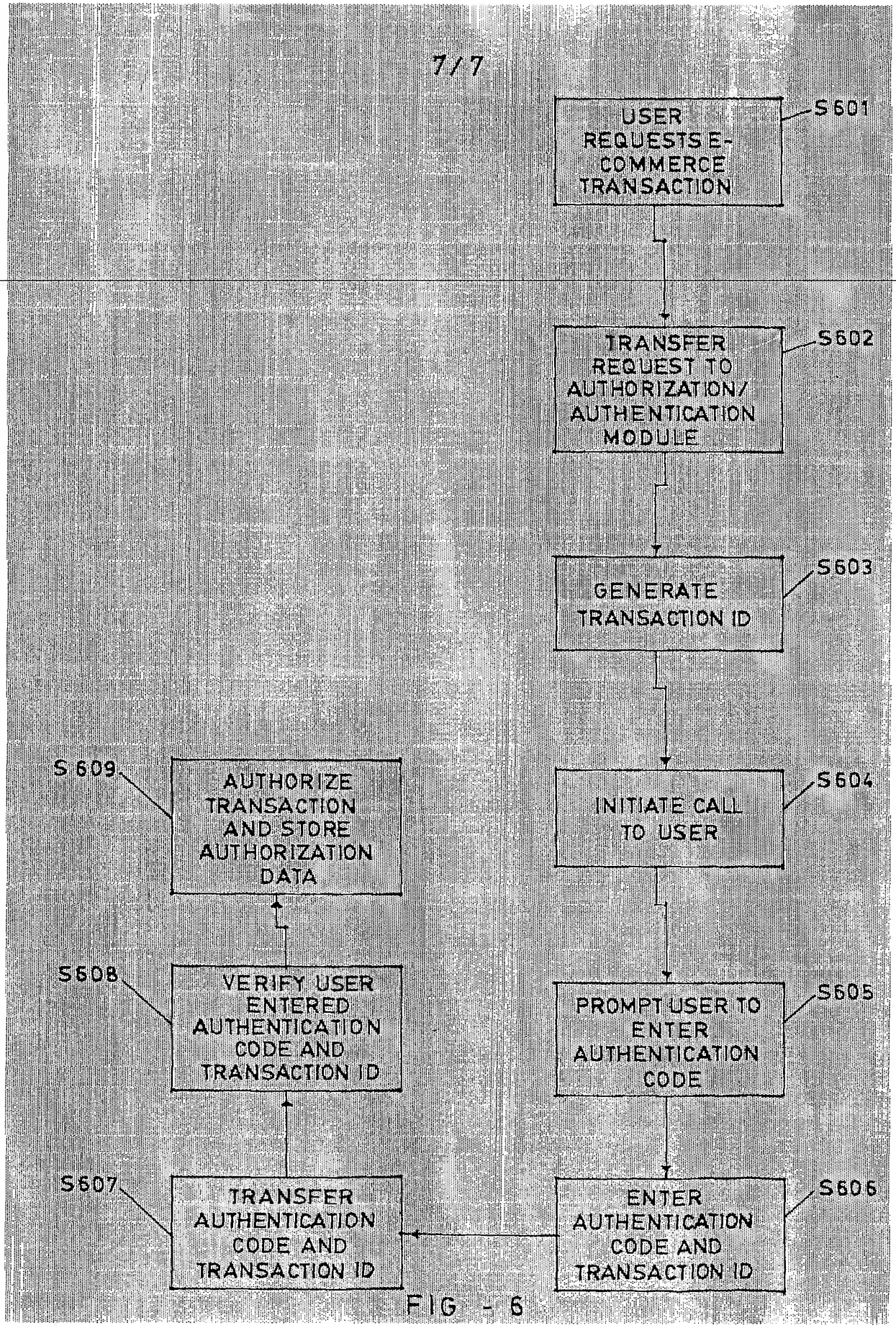


FIG - 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IN 01/00102

CLASSIFICATION OF SUBJECT MATTER

IPC[7]: H04L 9/32, 29/06, G06F 17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7]: G06F 7/10, 17/60, H04L 9/00, 9/32, 29/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1026644 A1 (APPAGE CORP. et al.) 9 August 2000 (09.08.00) *figs. 3,4; claims 1-6,15,18,19,34.*	1,2,4-7
A		9,10
A	US 5903721 A (SIXTUS T.) 11 May 1999 (11.05.99) *fig.2, claim 1.*	1,2,4,5,7,8

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
„A" document defining the general state of the art which is not considered to be of particular relevance
„E" earlier application or patent but published on or after the international filing date
„L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
„O" document referring to an oral disclosure, use, exhibition or other means
„P" document published prior to the international filing date but later than the priority date claimed
„T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
„X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
„Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 November 2001 (30.11.2001)	17 January 2002 (17.01.2002)
Name and mailing adress of the ISA/AT Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna Facsimile No. 1/53424/535	Authorized officer FUSSY Telephone No. 1/53424/328

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/IN 01/00102

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP A1 1026644	09-08-2000	AU A1 14692/99	03-08-2000
		US A 5903878	11-05-1999
US A 5903721	11-05-1999	AU A1 65494/98	29-09-1998
		EP A2 1008022	14-06-2000
		EP TD 1008022	25-01-2001
		ES T1 2150892	16-12-2000
		IL A0 131874	19-03-2001
		JP T2 01518212	09-10-2001
		NO A0 994428	13-09-1999
		NO A 994428	09-11-1999
		WO A2 9840809	17-09-1998
		WO A3 9840809	30-12-1998

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 322 091 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
25.06.2003 Bulletin 2003/26

(51) Int Cl.[7]: **H04L 29/06**

(21) Application number: **02258074.0**

(22) Date of filing: **22.11.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **19.12.2001 JP 2001385869**

(71) Applicant: **CANON KABUSHIKI KAISHA**
Tokyo (JP)

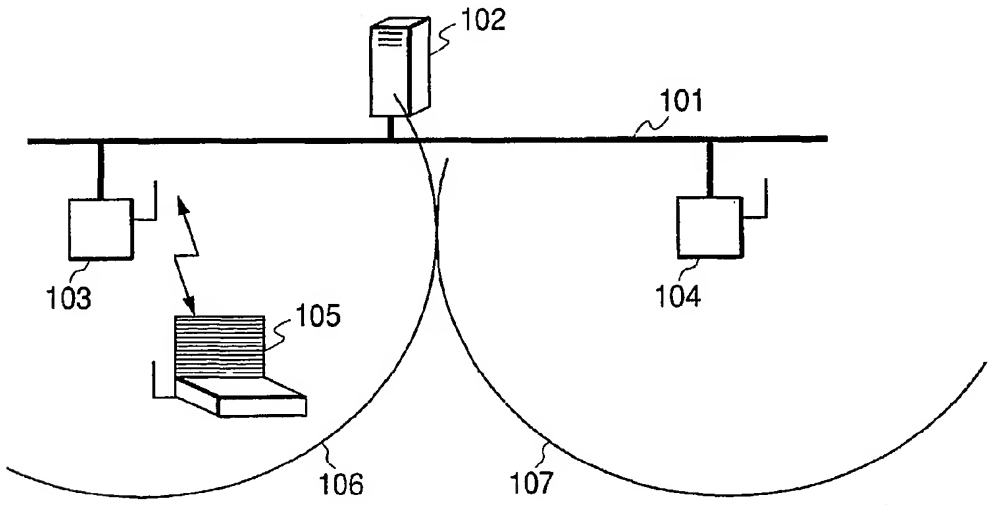
(72) Inventor: **Arai, Shunji,**
c/o Canon Kabushiki Kaisha
Tokyo (JP)

(74) Representative:
Beresford, Keith Denis Lewis et al
BERESFORD & Co.
2-5 Warwick Court,
High Holborn
London WC1R 5DH (GB)

(54) Communication system, server device, client device and method for controlling the same

(57) When a client server is permitted to be connected to a network through a first access point based on authentication by an authentication server, the authentication server informs the first access point of an encipher key such as a WEP key used for encipher communication between the client device and the first access point. Then, when the client device is moved to a communicable range of a second access point, the authentication server creates no new encipher keys but informs the second access point of the encipher key used for the encipher communication with the first access point, whereby encipher communication is executed between the client device and the second access point by using the same encipher key as that used for the encipher communication with the first access point.

FIG. 1



EP 1 322 091 A1

Description

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates to a communication system, in which a server device informs an access point of an encipher key used when a client terminal performs communication through the access point.

Description of the Related Art

[0002] Conventionally, in a wireless LAN system, a client terminal has been connected to a network through wireless communication with an access point on the network.

[0003] There is also a wireless LAN system, in which a client terminal receives authentication of connection to a network through an access point from an authentication server on a network.

[0004] In such a system, when the client terminal receives authentication from the authentication server, the client terminal and the authentication server create an encipher key of a wired equivalent privacy (WEP) encipher system, and the authentication server informs the access point of the created encipher key. Then, the client terminal transfers enciphered data with the access point by using the encipher key of the WEP encipher system to perform secure wireless communication.

[0005] Incidentally, a communicable range of the access point is limited to a range reached by electric waves. On the other hand, the client terminal can be freely moved. Accordingly, the client terminal may be moved from a communicable range of an access point 1 to a communicable range of an access point 2. In this case, the client terminal must receive authentication of connection to the network from the authentication server again through wireless communication with the access point 2, the client terminal and the authentication server must create a new WEP key, and the authentication server must inform the access point 2 of the new WEP key.

[0006] That is, when the client terminal changed the access point, re-authentication from the authentication server, creation of a new WEP key, informing of a WEP key, and the like prolonged the process until communication became possible. Consequently the process took time.

[0007] In addition, in a system of many client terminals, since authentication and creation of a WEP key prolonged a process, a load on an authentication server inevitably became large.

[0008] Furthermore, since the process took time when the access point was changed, usability was reduced.

SUMMARY OF THE INVENTION

[0009] A concern of the present invention is to improve usability of a system and a device.

[0010] Another concern of the present invention is to shorten time until communication becomes possible when a client terminal changes an access point.

[0011] Yet another concern of the present invention is to reduce a process when a client terminal changes an access point.

[0012] Other features of the present invention will become apparent upon reading of detailed description and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013]

FIG. 1 is a configuration view of a system according to an embodiment of the present invention.
FIG. 2 is a block diagram of an access point according to the embodiment of the invention.
FIG. 3 is a block diagram of a client terminal according to the embodiment of the invention.
FIG. 4 is a sequential view showing a system operation according to the embodiment of the invention.
FIG. 5 is a sequential view of the system operation according to the embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0014] Next, description will be made of an embodiment of the present invention.

[0015] FIG. 1 is a configuration view of a system according to the embodiment of the invention.

[0016] A reference numeral 101 denotes a network, to which an access point A103, and an access point B104 are connected. The two access points are shown in FIG. 1, but the number of installed points is not limited to two. Each of the access points A103 and B104 can perform wireless communication with a client terminal 105 present in communicable ranges 106, 107. According to the embodiment, as a wireless communication system, a wireless local area network (LAN) based on a standard such as IEEE 802. 11, IEEE 802. 11b, or IEEE 802. 11a is used.

[0017] The reference numeral 105 is the client terminal, which is connected to the network 101 through wireless communication with the access point A103 or B104. Though not shown in FIG. 1, a plurality of client terminals 105 may be present.

[0018] A reference numeral 102 denotes an authentication server, which authenticates the client terminal 105 connected to the network 101, and creates an encipher key used in a wired equivalency privacy (WEP) encipher system.

[0019] FIG. 2 is a block diagram of the access point

A103.

[0020] A case of the access point B104 is similar.

[0021] A reference numeral 201 denotes a wireless unit, which transfers wireless data. The wireless unit 201 is constituted of a transmission unit 210, a reception unit 211, and an antenna 212.

[0022] A reference numeral 202 denotes a signal process unit, which detects a signal received by the reception unit 211 to convert it into a digital signal, and modulates the signal in order to transmit a digital signal sent from a data process unit 203 by wireless. In addition, the signal process unit 202 has a function of adding a header or the like in order to use data sent from the data process unit 203 for wireless transmission, and removing a header or the like from received data to send it to the data process unit 203.

[0023] The reference numeral 203 is the data process unit, which is constituted of a transmission data process unit 205 for enciphering data from a network interface 208 by a WEP encipher system, and a reception data process unit 206 for decoding enciphered data.

[0024] A reference numeral 204 denotes a control unit, which executes determination of presence of a new client terminal 105, control of the entire access point A103, and the like.

[0025] A reference numeral 207 denotes a storage unit, which stores an encipher key for WEP enciphering, and information regarding an ID or the like of the client terminal 105.

[0026] The reference numeral 208 is the network interface, which is an interface between the access point A103 and the network 101.

[0027] FIG. 3 is a block diagram of the client terminal 105.

[0028] The client terminal 105 of the embodiment is constituted of a wireless communication card.

[0029] Functions similar to those of the access point A103 shown in FIG. 2 are denoted by similar numerals.

[0030] A reference numeral 301 denotes a data communication interface, which is connected to an information processor such as a personal computer to perform data communication.

[0031] A reference numeral 302 denotes a storage unit, which stores an encipher key for WEP enciphering, and information regarding an ID or the like of the client terminal 105 necessary for wireless communication with the access point A103 or the access point B104. According to the embodiment, as an ID of the client terminal 105, a media access control (MAC) address is used.

[0032] Next, description will be made an operation of the entire system of the embodiment with reference to the drawings.

[0033] First, a process of first connection of the client terminal 105 to the network 101 through the access point A103 is explained by referring to a sequential view of FIG. 4.

[0034] The client terminal 105 executes open authentication in the wireless LAN to be connected to the access point A103 (S401).

[0035] The access point A103 obtains an ID of the client terminal 105 (S402).

[0036] The access point A103 informs the authentication server 102 of the ID of the client terminal 105 (S403).

[0037] The authentication server 102 determines whether authentication for the connection of the client terminal 105 to the network 101 has been finished or not, based on the ID informed from the access point A103 (S404). The client terminal 105 makes the connection for the first time, and the authentication has not been finished. Thus, it is determined that the authentication has not been finished.

[0038] The authentication server 102 requests the client terminal 105 to input a user name and a password (S405).

[0039] The client terminal 105 inputs the user name and the password (S406).

[0040] In order to enhance secrecy of the user name and the password inputted in step S406, the client terminal 105 executes irreversible numerical value processing called one-way hash, and informs the authentication server 102 of its one-way hash data (S407).

[0041] The authentication server 102 collates the one-way hash data informed in step S407 with a data group regarding a user for permitting connection to the network 101, which is saved in a database in the authentication server 102. If a result of the collation shows coincident data, the connection to the network 101 is permitted to the client terminal 105, and the ID of the client terminal 105 is stored (step S408).

[0042] The client terminal 105 and the authentication server 102 create an encipher key called a WEP session key (S409). The WEP session key is an encipher key, which is used in the WEP encipher system, and valid only for enciphering traffic of the client terminal 105.

[0043] The authentication server 102 stores the created WEP session key in association with the ID of the client terminal 105, and informs it to the access point A103 (S410).

[0044] The access point A103 enciphers a broadcast key with the WEP session key (S411), and sends the enciphered broadcast key to the client terminal 105 (S412). The broadcast key is an encipher key, which is used when data broadcast from the access point A130 to a plurality of client terminals 105 is enciphered.

[0045] The client terminal 105 decodes the enciphered broadcast key by using the WEP session key created in step S409 to obtain a broadcast key (S413).

[0046] The access point A103 and the client terminal 105 start WEP encipher sequences (S414, S415).

[0047] Then, in communication with one client terminal 105 (point-to-point communication, the access point A103 transfers data enciphered with the WEP session key to perform secure wireless communication (S416). In broadcast communication with a plurality of client terminals 105 (point-to-multipoint communication), the ac-

cess point A103 transfers data enciphered with the broadcast key to perform secure wireless communication (S416).

[0048] Fig. 5 shows a sequential view of an operation when the client terminal 105, for which authentication of its connection to the network 101 through the access point A103 has been finished, is moved from the communicable range 106 of the access point A103 to the communicable range 107 of the access point B104 to be connected to the network 101 through the access point B104.

[0049] The client terminal 105 is moved out of the communicable range 106 of the access point A103 to be incommunicable with the access point A103 (S501). Then, the client terminal 105 is moved into the communicable range 107 of the access point B104 to be communicable with the access point B104.

[0050] The client terminal 105 executes open authentication to be connected to the access point B104 (S502).

[0051] The access point B104 obtains an ID of the client terminal 105 (S503).

[0052] The access point B104 informs the authentication server 102 of the ID of the client terminal 105 (S504).

[0053] The authentication server 102 determines whether authentication for the connection of the client terminal 105 to the network 101 has been finished or not, based on the ID informed in step S504, and the stored ID of the client terminal 105, for which the authentication has been finished (S505). Here, for the client terminal 105, the authentication of its connection to the network 101 through the access point A103 was finished in step S408 (FIG. 4), and the ID of the client terminal has been stored. Thus, it is determined that the authentication has been finished.

[0054] The authentication server 102 instructs the access point A103 to delete the WEP session key stored in the storage unit 207 to be used for wireless communication with the client terminal 105 (S506).

[0055] The authentication sever 102 informs the access point B104 of the WEP session key stored in association with the ID of the client terminal 105 in step S410 (FIG. 4) (S507).

[0056] The access point B104 enciphers a broadcast key with the WEP session key informed in step S507 (S508), and sends the enciphered broadcast key to the client terminal 105 (S509).

[0057] The client terminal 105 decodes the enciphered broadcast key by the WEP session key created in step S409 (FIG. 4) to obtain a broadcast key (S510).

[0058] The access point B104 and the client terminal 105 start WEP encipher sequences (S511, S512).

[0059] Then, in communication with one client terminal 105 (point-to-point communication), the access point B104 transfers data enciphered with the same WEP session key as that used for the communication between the client terminal 105 and the access point A103 to perform secure wireless communication (S513). In broadcast communication with a plurality of client terminals 105 (point-to-multipoint communication), the access point B104 transfers data enciphered with the broadcast key to perform secure wireless communication (S513).

[0060] In the embodiment, in step S507, the WEP session key stored in the authentication server 102 is informed to the access point B104. However, the WEP session key stored in the access point A103 may be informed through the authentication server 102 to the access point B104.

[0061] In the foregoing explanation, the client terminal 105 was the wireless communication card. However, a function similar to the wireless communication card may be incorporated in a personal computer or personal digital assistants (PDA).

[0062] Needless to say, the object of the present invention can be achieved by supplying a storage medium, in which software program codes for realizing the functions of the client terminal, the access points, and the authentication server are stored, to a system or a device, and causing the system or a computer (alternatively CPU or MPU) of the device to read and execute the program codes stored in the storage medium.

[0063] In such a case, the program codes read from the storage medium realize the functions of the embodiment themselves, and the storage medium, in which the program codes are stored, constitutes the present invention.

[0064] As the storage medium for supplying the program codes, a ROM, a floppy disk, a hard disk, an optical disk, a magneto-optical disk, a CD-ROM, a CD-R, a magnetic tape, a nonvolatile memory card or the like can be used.

[0065] Needless to say, not only the case of realizing the functions of the embodiment by executing the program codes read by the computer, but also a case where based on instructions of the program codes, a part or all of the actual process is executed by an OS or the like working on the computer to realize the functions of the embodiment are included in the present invention.

[0066] Furthermore, needless to say, a case where the program codes read from the storage medium are written in a CPU or the like provided in a function extension board inserted into the computer or a function extension unit connected to the computer and, then, based on instructions of the program codes, the CPU or the like provided in the function extension board or the function extension unit executes a part or all of the actual process to realize the functions of the embodiment is included in the present invention.

[0067] As described above, according to the present invention, it is possible to enhance usability of the device.

[0068] It is possible to shorten time until communication becomes possible when the client terminal changes an access point.

[0069] Moreover, it is possible to reduce a process when the client terminal changes an access point.

Claims

1. A communication system comprising:

   creation means for creating an encipher key used for communication between a client terminal and a first access point when the client terminal is permitted to be connected to a network through the first access point; and
   informing means for informing the first access point of the encipher key created by the creation means,

   wherein the informing means informs a second access point of the same encipher key as that informed to the first access point when the client terminal is connected to the network through the second access point.

2. A server device comprising:

   creation means for creating an encipher key used for communication between a client terminal and a first access point when the client terminal is permitted to be connected to a network through the first access point; and
   informing means for informing the first access point of the encipher key created by the creation means,

   wherein the informing means informs a second access point of the same encipher key as that informed to the first access point when the client terminal is connected to the network through the second access point.

3. The server device according to claim 2, further comprising: instruction means for instructing the first access point to delete the encipher key when the client terminal is connected to the network through the second access point.

4. The server device according to claim 2, wherein the encipher key which the informing means informs to the second access point is an encipher key stored when the encipher key is created by the creation means, or an encipher key received from the first access point.

5. A server device for informing an access point of an encipher key used when a client terminal performs communication through the access point, comprising:

   determination means for determining transition of the client terminal from communication through a first access point to communication through a second access point; and
   informing means for informing the second access point of the same encipher key as that informed to the first access point based on the determination of the determination means.

6. A server device comprising:

   authentication means for authenticating connection of a client device to a network through an access point;
   informing means for informing an access point, to which the client device is connected, of an encipher key in accordance with a result of the authentication by the authentication means; and
   determination means for determining whether the client device which requests the authentication means to execute authentication is a client device or not, for which authentication has been finished,

   wherein the informing means informs the access point, to which the client device is connected, of a new encipher key in accordance with the determination of the determination means.

7. The server device according to claim 6, wherein the informing means informs the access point, to which the client device is connected, of a new encipher key if the determination means determines that the client device which requests the authentication has been unauthenticated, and the access point, to which the client device is currently connected, of the same encipher key as that informed to an access point in previous authentication if it is determined that the client device is the client device, for which the authentication has been finished.

8. A client terminal connected to a network through an access point, comprising:

   creation means for creating an encipher key used for communication with a first access point; and
   communication means for executing encipher communication with the first access point by using the encipher key created by the creation means,

   wherein the communication means uses the encipher key used for the encipher communication with the first access point even when an access point connected for connection to the network is changed from the first access point to a second ac-

cess point.

9. The client terminal according to claim 8, further comprising: receiving means for receiving a permission notice of the connection to the network from an authentication server,

wherein the creation means creates the encipher key in accordance with the reception of the permission notice by the receiving means.

10. A control method for a communication system, comprising the steps of:

creating an encipher key used for communication between a client terminal and a first access point when the client terminal is permitted to be connected to a network through the first access point; and
informing the first access point of the encipher key created by the creation means,

wherein in the informing step, a second access point is informed of the same encipher key as that informed to the first access point when the client terminal is connected to the network through the second access point.

11. A control method for a server device, comprising the steps of:

creating an encipher key used for communication between a client terminal and a first access point when the client terminal is permitted to be connected to a network through the first access point; and
informing the first access point of the encipher key created by the creation means,

wherein in the informing step, a second access point is informed of the same encipher key as that informed to the first access point when the client terminal is connected to the network through the second access point.

12. A control method of a server device for informing an access point of an encipher key used when a client terminal performs communication through the access point, comprising the steps of:

determining transition of the client terminal from communication through a first access point to communication through a second access point; and
informing the second access point of the same encipher key as that informed to the first access point based on the determination of the determination step.

13. A control method for a server device, comprising the steps of:

authenticating connection of a client device to a network through an access point;
informing an access point, to which the client device is connected, of an encipher key in accordance with a result of the authentication in the authentication step; and
determining whether the client device which requests authentication in the authentication step is a client device or not, for which authentication has been finished,

wherein in the informing step, the access point, to which the client device is connected, is informed of a new encipher key in accordance with the determination in the determination step.

14. A control method for a client terminal connected to a network through an access point, comprising the steps of:

creating an encipher key used for communication with a first access point; and
executing encipher communication with the first access point by using the encipher key created in the creation step,

wherein in the communication step, the encipher key used for the encipher communication with the first access point is used even when an access point connected for connection to the network is changed from the first access point to a second access point.

FIG. 1

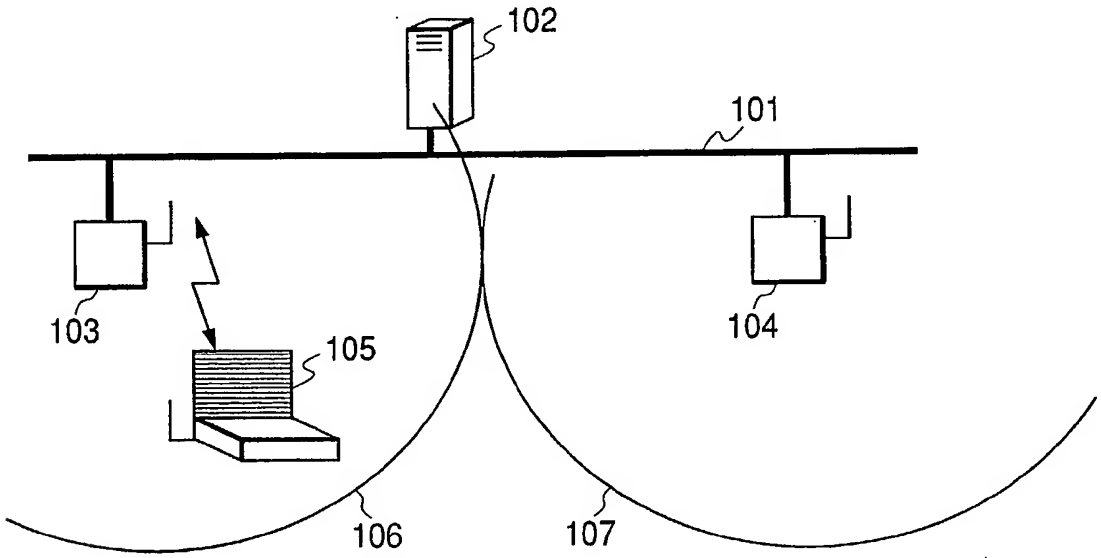


FIG. 2

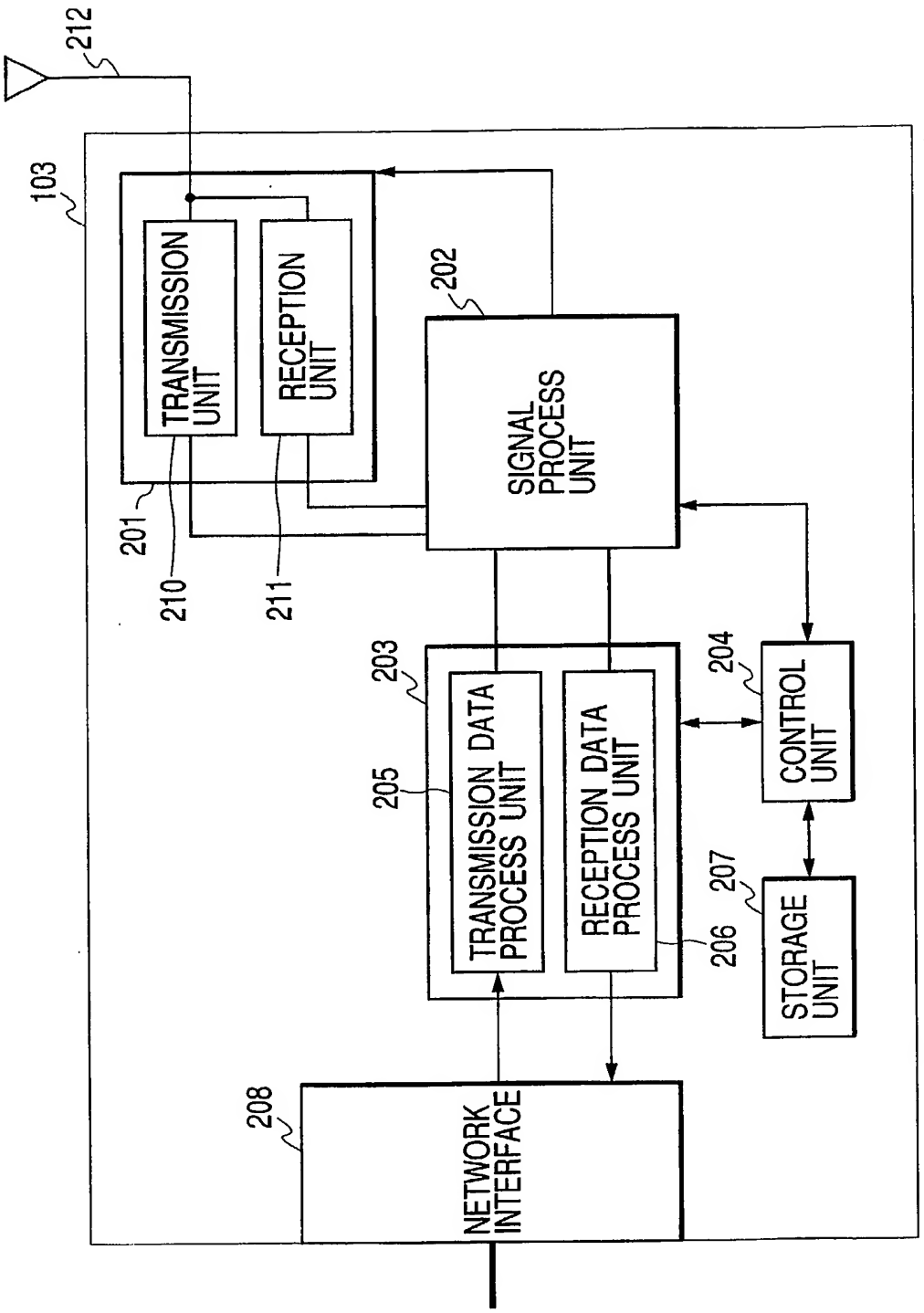


FIG. 3

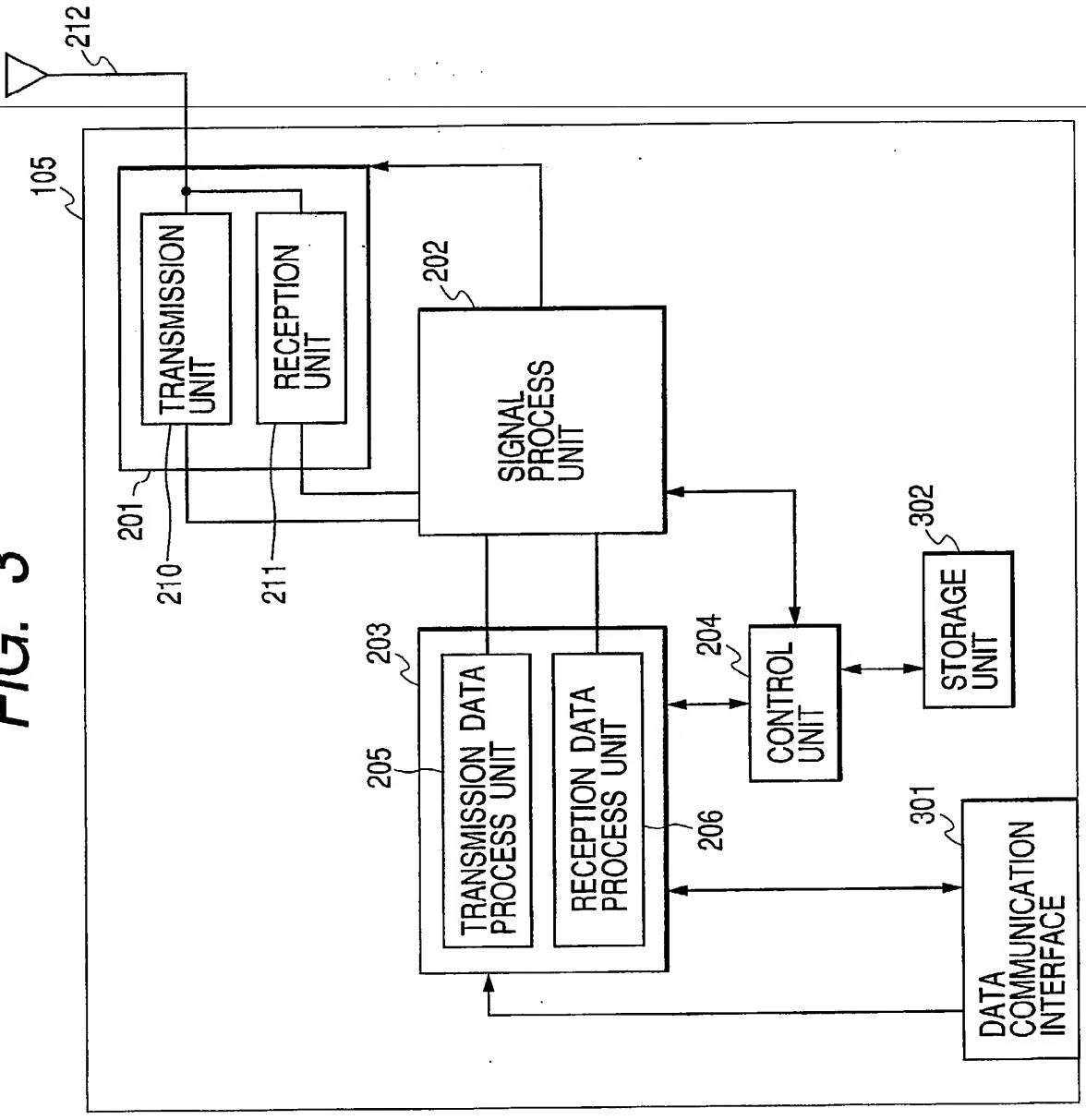


FIG. 4

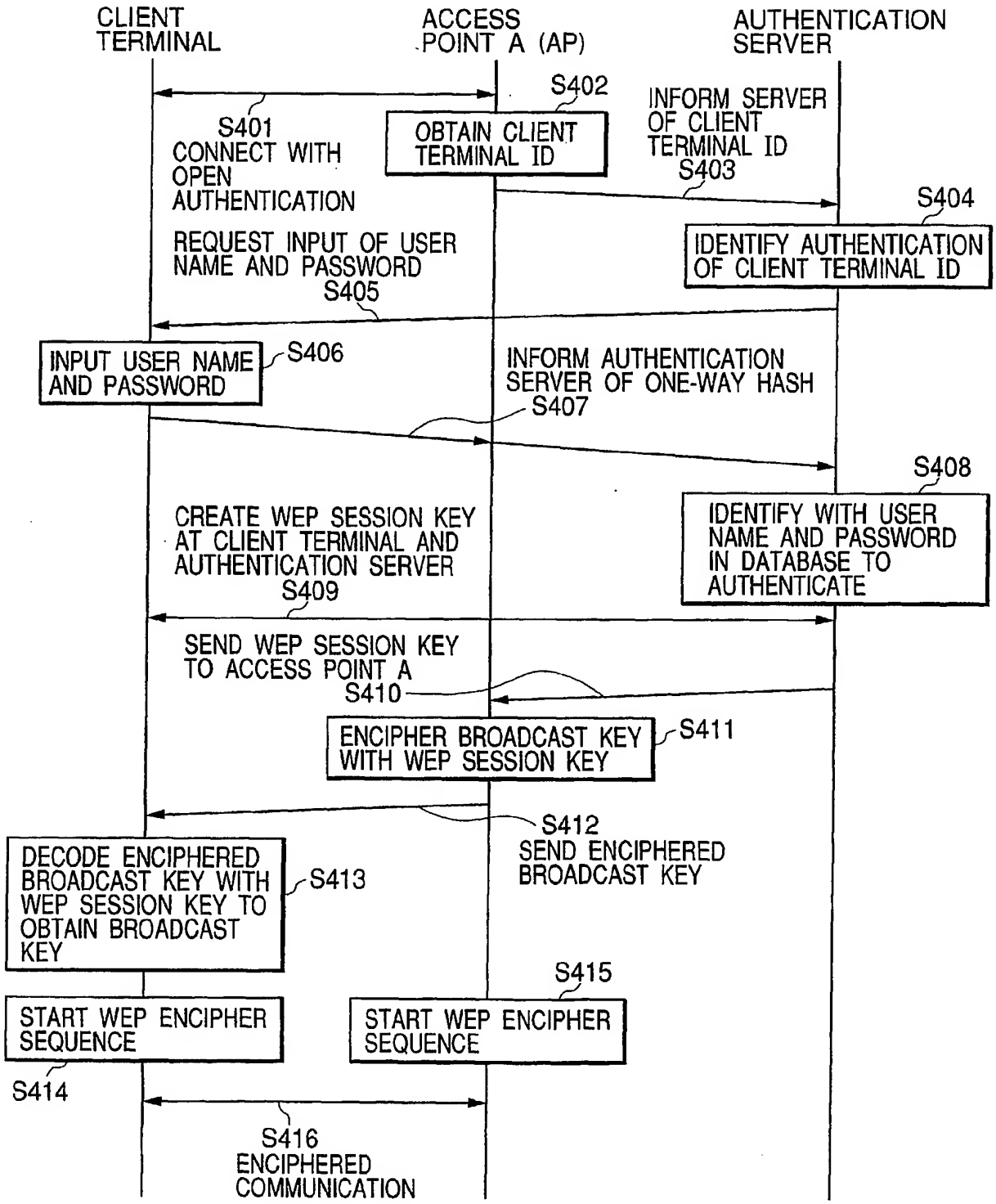
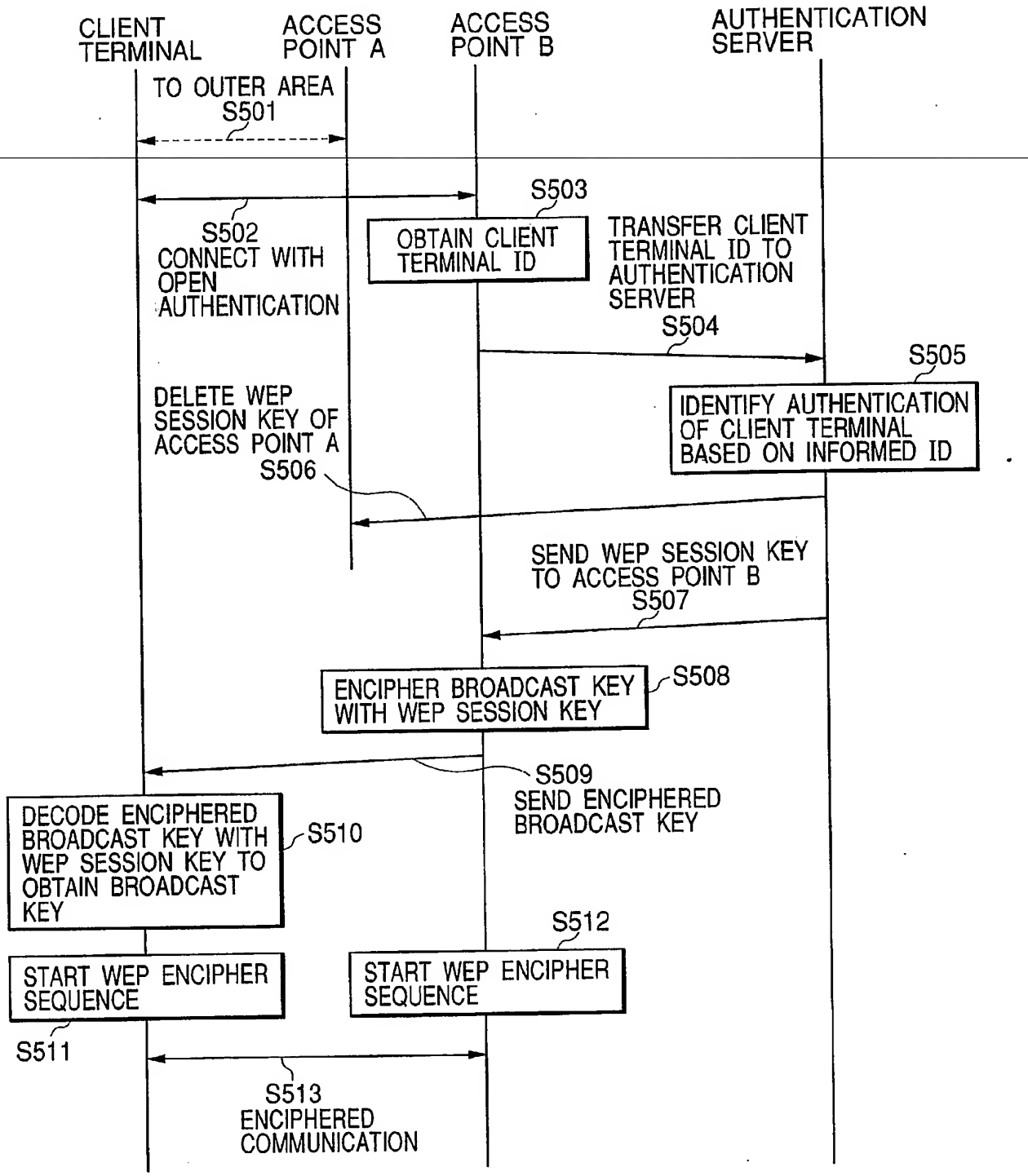


FIG. 5



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 25 8074

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
P,X	WO 02 096151 A (FLARION TECHNOLOGIES INC ;VANDERVEEN MICHAELA CATALINA (US)) 28 November 2002 (2002-11-28) * abstract * * page 9, line 19 - line 20 * * page 11, line 21 - line 26 * * page 13, line 5 - line 8 * * page 13, line 24 - page 14, line 6 * * page 14, line 21 - line 28 * * page 15, line 7 - line 19 * * page 19, line 5 - line 23 * * figures 2-7 *	1,8-10, 14	H04L29/06
X	WO 01 24560 A (SIMOCO INT LTD ;RAYNE MARK WENTWORTH (GB)) 5 April 2001 (2001-04-05) * page 7, line 28 - page 8, line 8 *	8,9,14	
A	WO 01 22685 A (ERICSSON TELEFON AB L M) 29 March 2001 (2001-03-29) * page 2, line 32 - page 4, line 15 * * page 4, line 14 - page 5, line 32 * * page 7, line 21 - page 8, line 16 * * page 11, line 1 - page 13, line 27 *	1-14	
A	T. TANAKA,M.MORIKURA,H.TAKANASHI: "Nomadic Computing Environment Employing Wired and Wireless Networks" IEICE TRANS. COMMUN., vol. E81-B, no. 8, 12 January 1998 (1998-01-12), XP000788462 * page 1569, right-hand column, line 14 - page 1571, right-hand column, line 47 *	1-14	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
H04L
H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	23 April 2003	Olaechea, F

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 25 8074

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

23-04-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 02096151 A	28-11-2002	WO 02096151 A1	28-11-2002
		US 2002197979 A1	26-12-2002
WO 0124560 A	05-04-2001	AU 7534900 A	30-04-2001
		WO 0124560 A1	05-04-2001
		GB 2359464 A	22-08-2001
WO 0122685 A	29-03-2001	SE 519471 C2	04-03-2003
		AU 7694200 A	24-04-2001
		WO 0122685 A1	29-03-2001
		SE 9903370 A	21-03-2001

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82